UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO
DEPARTAMENTO DE MATEMÁTICA
PROGRAMA DE PÓS GRADUAÇÃO EM MATEMÁTICA

Gislayni Telles Vieira Santana Lopes

A CONJECTURA DE EULER SOBRE SOMAS DE POTÊNCIAS QUÁRTICAS DE NÚMEROS INTEIROS

VITÓRIA
2017

Gislayni Telles Vieira Santana Lopes

A CONJECTURA DE EULER SOBRE SOMAS DE POTÊNCIAS QUÁRTICAS DE NÚMEROS INTEIROS

Dissertação apresentada ao Programa de Pós Graduação em Matemática da Universidade Federal do Espírito Santo - PPGMAT, UFES - como requisito parcial para a obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. José Gilvan de Oliveira.

VITÓRIA

2017

Dedicatória

Ao meu esposo André, meus pais Conceição e José e aos meus irmãos Carlos, Charleston, Charlie e minha irmã Charlene. Vocês são a minha base. A minha maior riqueza.

Agradecimentos

Agradeço primeiramente a Deus, que me sustentou até aqui. Nos momentos difíceis, Ele foi a minha força. Sou grata a Ele por ter me dado a chance de ter essa oportunidade na minha vida.

Agradeço ao meu amado esposo, meu ajudador e meu maior motivador. Minha inspiração. Faltam-me palavras para expressar o quanto você foi essencial nessa conquista.

Agradeço a minha família, em especial aos meus pais, pela determinação e luta na minha formação acadêmica. Essa conquista não seria possível sem o apoio de vocês.

Agradeço aos meus irmãos e amigos, que muito compreenderam minha ausência. Em especial, minha amiga Pollyanna, pelo incentivo e sábios conselhos.

Agradeço ao meu orientador, prof. Dr. José Gilvan de Oliveira, pela orientação, dedicação e paciência durante o processo de realização desse trabalho.

Agradeço a CAPES, pelo apoio financeiro.

Resumo

Em 1772, Leonard Euler conjecturou que a soma de n potências de números inteiros positivos de um dado expoente n também seria uma tal potência. Contudo, se o número de potências nessa soma fosse inferior ao expoente, então tal soma não poderia resultar em uma potência de expoente n. No presente trabalho vamos nos concentrar no caso $n = 4$ da Conjectura de Euler. Numa primeira abordagem, vamos apresentar um contraexemplo para a conjectura, ou seja, vamos exibir solução inteira positiva para a equação diofantina $a^4 + b^4 + c^4 = e^4$, que é equivalente a verificar que o conjunto dos pontos racionais da superfície $S_1 \colon r^4 + s^4 + t^4 = 1$ é não vazio. Usaremos a teoria de curvas elípticas e conceitos da Teoria dos Números, como a reciprocidade quadrática e o teorema de Legendre, na construção de um método para obter o contraexemplo. Em uma segunda abordagem, usaremos a estrutura de grupo de uma curva elíptica para mostrar que existe uma infinidade de soluções inteiras positivas para a equação diofantina acima, se acrescentarmos uma quarta potência de um número inteiro nessa soma.

Palavras-chaves: Conjectura de Euler. Curvas Elípticas. Equações Diofantinas.

Abstract

In 1772, Leonard Euler conjectured that the sum of n powers of positive integers of a given exponent n would also be such a power. However, if the number of powers in this sum is less than the exponent, then such sum could not result in an exponent power n. In the present work we will focus on the $n = 4$ case of the Euler's conjecture. In a first approach, we will present a counterexample to the conjecture, that is, we will display positive whole solution for the diophantine equation $a^4 + b^4 + c^4 = e^4$, which is equivalent to verify that the set of rational points of the surface $S_1 : r^4 + s^4 + t^4 = 1$ is not empty. We will use the theory of elliptic curves and concepts of Number Theory, such as quadratic reciprocity and Legendre's theorem, in the construction of a method to obtain the counterexample. In a second approach, we will use the group structure of an elliptic curve to show that there is an infinity of positive integer solutions for the above Diophantine equation if we add a quartic power of an integer in that sum.

Key-words: Euler Conjecture. Elliptic Curves. Diophantine Equations.

Sumário

Capítulo 1

Introdução

Um dos principais problemas na Teoria dos Números é encontrar soluções inteiras para equações diofantinas. O conhecido teorema de Pitágoras afirma que em um triângulo retângulo qualquer a soma dos quadrados dos dois catetos é o quadrado da hipotenusa do triângulo. Já o último teorema de Fermat considera o expoente como sendo um número inteiro maior do que 2 na fórmula de Pitágoras e afirma que nesse caso, a equação não tem solução inteira não trivial. Este resultado foi provado por Andrew Wiles em 1994, cerca de 350 anos após ter sido enunciado. Em 1772, a partir dos seus resultados parciais sobre o problema de Fermat para o caso de expoente $n = 3$, Leonard Euler conjecturou que seriam necessários pelo menos n potências com expoente n de números inteiros positivos para que a soma resultasse em uma tal potência.
Esta afirmação matemática foi uma das mais famosas conjecturas no campo da álgebra, que perdurou cerca de dois séculos. Inicialmente, em 1966, usando recurso computacional, L. J. Lander e T. R. Parkin encontraram um contraexemplo dessa conjectura para o caso do expoente $n = 5$, a saber

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5$$

Contudo as técnicas computacionais usadas por eles não foram suficientes para resolver o problema no caso $n = 4$. Posteriormente, em 1988 Noam Elkies, usando a teoria de curvas elípticas, obteve o seguinte contraexemplo para o caso $n = 4$:

$$2682440^4 + 15365639^4 + 18796760^4 = 20615673^4.$$

No presente trabalho, vamos nos concentrar no caso $n = 4$ da conjectura de Euler. Mais precisamente, vamos exibir números inteiros positivos satisfazendo a equação diofantina

$$a^4 + b^4 + c^4 + d^4 = e^4 \tag{1.1}$$

considerando inicialmente o caso em que uma das variáveis é nula, e posteriormente, o caso em que todas as variáveis são diferentes de zero.

No Capítulo 4, trataremos da primeira abordagem: mostraremos como N. Elkies obteve o contraexemplo acima mencionado da conjectura de Euler. Faremos a conexão entre a Geometria Algébrica, no estudo de curvas e superfícies, com a Teoria dos Números, no estudo de soluções inteiras de equações diofantinas, pois buscar soluções inteiras para a primeira equação estudada é equivalente a buscar pontos racionais $(r, s, t) = (a/e,\ b/e,\ c/e)$ para a superfície $r^4+s^4+t^4 = 1$. Com esse objetivo usaremos a aritmética das curvas elípticas, o teorema de Legendre e a Lei da reciprocidade quadrática, na construção de um método para encontrar números inteiros positivos satisfazendo a equação (1.1). A referência básica deste capítulo é o artigo [4].

No Capítulo 5 trataremos da segunda abordagem: Vamos mostrar como Lee W. Jacobi e Daniel J. Madden desenvolveram um método para gerar uma sequência infinita de soluções inteiras positivas para a equação (1.1) considerando o caso particular em que $e = a + b + c + d$. Isto foi possível porque uma solução particular, encontrada por Simcha Brudno ([1]) em 1964,

$$5400^4 + 1770^4 + 2634^4 + 955^4 = 5491^4,$$

também satisfaz

$$5400 + 1770 + 955 = 2634 + 5491.$$

Isto significa que $(5400, 1770, -2634, 955)$ é uma solução da equação diofantina

$$a^4 + b^4 + c^4 + d^4 = (a + b + c + d)^4. \tag{1.2}$$

Vale ressaltar que até antes da publicação de Jacobi e Madden, não era conhecido um método que fornecesse uma solução paramétrica para a equação (1.2) considerando todas as variáveis diferentes de zero.

Mostraremos que o conjunto dos números inteiros positivos que satisfazem a equação (1.2) está associado com os pontos racionais em uma curva elíptica específica. Usaremos o teorema de Mazur para mostrar que a partir de um ponto particular nessa curva, conseguimos uma infinidade de soluções inteiras positivas para a equação (1.2). A referência básica para este capítulo é o artigo [6].

No Capítulo 2 estudaremos conceitos necessários da Geometria Algébrica, a fim de contextualizar o nosso objeto de estudo, tais como: curvas algébricas, plano projetivo, parametrizações,

interseções entre curvas, em destaque o teorema de Bezout, que determina o número de pontos na interseção entre duas curvas algébricas planas.

No Capítulo 3 daremos destaque à teoria de curvas elípticas. Tais curvas são particularmente interessantes porque possuem uma estrutura aritmética bastante rica, em especial, o conjunto dos pontos racionais sobre uma dada curva elíptica admite estrutura de grupo abeliano. Veremos importantes resultados que fornecem uma caracterização para esse grupo, em destaque os teoremas de Mordell-Weil e Mazur.

Capítulo 2

Curvas Algébricas

No presente capítulo estudaremos conceitos necessários para contextualização do nosso objeto de estudo, tais como variedades afins e projetivas, dimensão, funções regulares, curvas e superfícies algébricas. No decorrer deste capítulo, k denotará um corpo algebricamente fechado, a menos que se mencione o contrário. Nossas referências básicas serão os textos [7], [9] e [10].

2.1 Curvas Algébricas Afins e Projetivas

2.1.1 Variedades Afins

Denotamos por $\mathbb{A}_k^n$ ou simplesmente $\mathbb{A}^n$, o conjunto de todas as n-uplas dos elementos do corpo k, chamado *espaço afim* de dimensão n sobre k. Um elemento $P = (a_1, a_2, ..., a_n) \in \mathbb{A}^n$ é chamado um ponto e $a_i,\ 1 \leq i \leq n$, é a i-ésima coordenada de P. Sejam $k[x_1, x_2, ..., x_n]$ o anel de polinômios em n variáveis com coeficientes em k e V um subconjunto de $\mathbb{A}^n$. Dizemos que V é um *conjunto algébrico* se existe um conjunto de polinômios $S \subset k[x_1, x_2, ..., x_n]$ tal que $V = V(S)$, onde

$$V(S) = \{P \in \mathbb{A}^n / f(P) = 0 \ \forall \ f \in S\}.$$

Em particular, quando S é formado por um único polinômio f, o conjunto $V(f)$ é chamado de *hipersuperfície*. Se f é um polinômio não constante no anel de polinômios $k[x_1, ..., x_n]$, sua decomposição em fatores irredutíveis $f = f_1^{a_1} f_2^{a_2} ... f_r^{a_r}$ induz a decomposição da hipersuperfície $V(f) = \cup\, V(f_i)$, $1 \leq i \leq r$, como união de hipersuperfícies. Os conjuntos $V(f_i)$, $1 \leq i \leq r$,, são

chamados componentes irredutíveis de $V(f)$. Dado um conjunto algébrico $V \subset \mathbb{A}^n$, o conjunto

$$I = I(V) = \{f \in k[x_1, x_2, ..., x_n] / f(P) = 0 \ \forall \ P \in V\}$$

é chamado o *ideal* de V. O Teorema da Base de Hilbert mostra que cada conjunto algébrico V é o conjunto das raízes comuns de uma quantidade finita de polinômios, isto é, $I(V)$ é gerado por uma quantidade finita de polinômios $f_1, f_2, ..., f_r \in k[x_1, x_2, ..., x_n]$. Dessa forma,

$$V = \{P \in \mathbb{A}^n / f_1(P) = f_2(P) = ... = f_r(P) = 0\}.$$

Um conjunto algébrico $V \subset \mathbb{A}^n$ é chamado *irredutível* se não pode ser escrito como $V = V_1 \cup V_2$, onde V_1 e V_2 são subconjuntos algébricos próprios de V. Caso contrário, V é redutível. Existe uma relação entre a geometria de um conjunto algébrico V com uma propriedade algébrica do seu ideal $I(V)$, esclarecida pela seguinte proposição.

Proposição 2.1.1. *Um conjunto algébrico $V \subset \mathbb{A}^n$ é irredutível se, e somente se, o ideal $I(V)$ é primo.*

Demonstração. i) Sejam V um conjunto algébrico irredutível, $f, g \in k[x_1, x_2, ..., x_n]$ polinômios sem fator comum, tais que $f.g \in I(V)$. Queremos mostrar que $f \in I(V)$ ou $g \in I(V)$. Temos que fg se anula em todos os pontos de V, dessa forma, $V \subset V(f) \cup V(g)$. Por outro lado, vale a seguinte igualdade

$$V = (V \cap V(f)) \cup (V \cap V(g)).$$

Pela irredutibilidade de V, um desses conjuntos, digamos $V \cap V(f)$, deve ser igual a V. Assim, $f \in I(V)$.

ii) Suponha que V não seja um conjunto algébrico irredutível. Existem V_1, V_2 subconjuntos algébricos próprios de V tais que $V = V_1 \cup V_2$. Assim, existem $f_1 \in I(V_1) \backslash I(V)$ e

$f_2 \in I(V_2) \backslash I(V)$ tais que $f = f_1 f_2 \in I(V)$, mas $f_1, f_2 \notin I(V)$. □

Definição 2.1.2. *Um conjunto algébrico irredutível $V \subset \mathbb{A}^n$ é chamado variedade algébrica afim.*

Exemplo 2.1.3. *$\mathbb{A}^n$ é uma variedade afim para todo n, pois o ideal $I(\mathbb{A}^n) = < 0 >$ é primo. Seja f um polinômio irredutível em $k[x_1, ..., x_n]$, então $V(f)$ é uma variedade afim. Se $n = 2$ então $V(f)$ é chamado de curva plana afim, se $n = 3$ então $V(f)$ é chamada de superfície afim.*

Definição 2.1.4. *Seja V uma variedade afim no espaço $\mathbb{A}^n$ sobre um corpo k. Uma aplicação $f : V \longrightarrow \mathbb{A}^1$ é chamada regular se existe um polinômio $F \in k[x_1, ..., x_n]$ tal que $f(P) = F(P)$ para todo $P \in V$.*

Note que o polinômio F não é unicamente determinado. De fato, dois polinômios F e G determinam a mesma função regular em V se e somente se $F(P)-G(P)=0$ para todo $P \in V$, ou seja, se e somente se, $F-G \in I(V)$. Dessa forma, o conjunto das funções regulares de V formam um anel

$$A[V] = k[x_1, ..., x_n]/I(V)$$

chamado *anel de coordenadas* de V. É claro que $A[V]$ é um domínio se e somente se $I(V)$ é um ideal primo, se e somente se V é uma variedade afim.

O corpo das funções racionais de uma variedade afim V, denotado por $k(V)$, é o corpo quociente do anel de coordenadas $A[V]$, isto é,

$$k(V) = \Big\{ \frac{g}{h} / \ g, \ h \ \in A[V], \ h \ \neq 0 \Big\}.$$

Dois elementos g_1/h_1 e g_2/h_2 representam a mesma função racional em $k(V)$ se $g_2h_1 - g_1h_2 \in I(V), \ g_1, \ g_2, \ h_1, \ h_2 \ \in A[V]$. A dimensão de V, denotada por $dim(V)$, é obtida através do grau de transcendência da extensão $k(V)/k$.

Exemplo 2.1.5. *Se $V = \mathbb{A}^n$ então $dim(V) = n$, pois $k(\mathbb{A}^n) = k(x_1, ..., x_n)$.*

Dada uma variedade $V \subset \mathbb{A}^n$, dizemos que a função racional $\varphi \in k(V)$ é regular ou que está definida no ponto $P \in V$, se admitir uma representação $\varphi = g/h$, com $g, \ h \ \in A[V]$ e $h(P) \neq 0$. Fixado um ponto P em V, pode-se definir o conjunto das funções racionais que estão definidas em P, chamado *anel local* de P em V,

$$\mathcal{O}_P(V) = \{\varphi \ \in k(V); \ \varphi \text{ é } regular \ em \ P\}.$$

Claramente, uma função regular é uma função racional definida em todos os pontos de V, assim, temos uma natural inclusão $A[V] \subset \mathcal{O}_P(V) \subset k(V)$ para todo P em V. Sejam $V \subset \mathbb{A}^n$ e $W \subset \mathbb{A}^m$ duas variedades afins. Uma aplicação $\varphi \colon V \longrightarrow \mathbb{A}^m$ é chamada uma *aplicação racional* se existem funções racionais $\Phi_1, \ \Phi_2, ..., \ \Phi_n$ tais que $\varphi(P) = (\Phi_1(P), \ \Phi_2(P), ..., \ \Phi_n(P))$ para todo P na interseção dos domínios de Φ_i. Além disso, se o conjunto $Im(\varphi) \subset W$, então φ é uma aplicação racional de V em W.

Definição 2.1.6. *Uma aplicação $\varphi \colon V \longrightarrow W$ é birracional se existe uma aplicação racional $\Psi \colon W \longrightarrow V$ tal que $\varphi \circ \Psi = Id_W$ e $\Psi \circ \varphi = Id_V$. Se existe uma tal aplicação de V em W, dizemos que V e W são birracionalmente equivalentes.*

Definição 2.1.7. *Uma aplicação racional de V em W, que é regular em todos os pontos de V é chamada morfismo. Um isomorfismo é um morfismo com um morfismo inverso.*

Exemplo 2.1.8. *Tomando $V = \mathbb{A}^1$ e $W = V(y - x^2) \subset \mathbb{A}^2$. A parametrização $f\colon V \longrightarrow W$ definida por $f(t) = (t, t^2)$ é um morfismo da variedade V em W, e a projeção $g\colon W \longrightarrow V$ definida por $g(x, y) = x$, é o morfismo inverso. Assim, as variedades V e W são birracionalmente equivalentes. Consequentemente, $A[V] \simeq A[W]$, pois*

$$A[\mathbb{A}^1] = k[x]/ < 0 > \simeq k[x] \text{ e } A[W] = k[x, y]/ < y - x^2 > \simeq k[x].$$

2.1.2 Variedades Projetivas

O *espaço projetivo* $\mathbb{P}^n_k$ ou simplesmente $\mathbb{P}^n$ de dimensão n sobre k é o conjunto das retas de k^{n+1} contendo a origem. Dado um ponto $P = (a_0, a_1, ..., a_n) \in k^{n+1}\backslash\{(0, 0, ..., 0)\}$, denotamos por $(a_0 : a_1 : ... : a_n)$ o ponto de $\mathbb{P}^n$ correspondente à reta de k^{n+1} determinada pela origem e o ponto P. Assim,

$$\mathbb{P}^n = k^{n+1}\backslash\{(0, 0, ..., 0)\}\Big/ \sim$$

onde $(a_0, a_1, ..., a_n) \sim (b_0, b_1, ..., b_n)$ se, e somente se, existe $\lambda \in k^*$ tal que $(b_0, b_1, ..., b_n) = (\lambda a_0, \lambda a_1, ..., \lambda a_n)$. Para cada i, seja

$$U_i = \{(a_0 : a_1 : ... : a_i : ... : a_n) \in \mathbb{P}^n;\ a_i \neq 0\}.$$

Existe uma natural inclusão $\varphi_i\colon \mathbb{A}^n \longrightarrow U_i$ definida pela aplicação

$$\varphi_i(a_1, ..., a_n) = (a_1 : ... : a_{i-1} : 1 : a_i : ... : a_n)$$

cuja inversa é definida por $\varphi_i^{-1}(a_0 : ... : a_n) = Q$, onde Q é o ponto de coordenadas afins

$$\Big(\frac{a_0}{a_i}, ..., \frac{a_n}{a_i}\Big),\ \text{omitir } \frac{a_i}{a_i}.$$

Note que φ_i^{-1} está bem definida, uma vez que a_j/a_i são independentes da escolha de coordenadas homogêneas. Para i fixo, identificamos $\mathbb{A}^n$ com o conjunto U_i via a aplicação φ_i,

O complementar $\mathbb{H}_n = \mathbb{P}^n\backslash U_n = \{(a_0 : a_1 : ... : a_n) \in \mathbb{P}^n/\ a_n = 0\}$, convencionalmente chamado *hiperplano no infinito*, pode ser identificado com $\mathbb{P}^{n-1}$ via a correspondência

$$(a_0 : ... : a_{n-1} : 0) \longleftrightarrow (a_0 : ... : a_{n-1}).$$

Consequentemente, $\mathbb{P}^n = U_n \cup H_n \simeq \mathbb{A}^n \cup \mathbb{P}^{n-1}$.

Definição 2.1.9. *Dizemos que um polinômio F em $k[x_0, x_1, ..., x_n]$ é homogêneo de grau d, se é uma soma de monômios $g = a\prod_{i=0}^{n} x_i^{d_i} \in k[x_0, x_1, ..., x_n]$, $a \neq 0$ e $d_0 + d_1 + ... + d_n = d$. De maneira equivalente, temos que F é homogêneo de grau d se, e somente se, $F(tx_0, tx_1, ..., tx_n) = t^d F(x_0, x_1, ..., x_n)$ para todo $t \in k$.*

Observação 2.1.10. *Dado um polinômio $F \in k[x_0, x_1, ..., x_n]\backslash k$ e um ponto*

$P = (a_0 : a_1... : a_n) \in \mathbb{P}^n$, o valor $F(P)$ pode não estar bem definido, pois as coordenadas homogêneas de um ponto $P \in \mathbb{P}^n$ não são unicamente determinadas. Assim, o conjunto $V(F)$ não pode ser definido da mesma forma do caso afim. Contudo, se F for um polinômio homogêneo de grau d, então $F(\lambda a_0, ..., \lambda a_n) = 0$ se, e somente se, para qualquer $\lambda \neq 0$, $\lambda^d F(a_0, a_1..., a_n) = 0$, de modo que a propriedade de $F(a_0, ..., a_n) = 0$, independe da escolha de coordenadas homogêneas $(a_0, ..., a_n)$.

Um ideal $I \subset k[x_0, ..., x_n]$ é homogêneo se é gerado por polinômios homogêneos.

Um conjunto $V \subset \mathbb{P}^n$ é um *conjunto algébrico projetivo* se existe um conjunto de polinômios homogêneos $S \subset k[x_0, x_1, ..., x_n]$ tal que

$$V = V(S) = \{P \in \mathbb{P}^n / F(P) = 0 \ \forall \ F \in \ S\}.$$

O ideal homogêneo $I(V) \subset k[x_0, x_1, ..., x_n]$ é gerado pelos polinômios homogêneos $F \in S$ que satisfazem a equação $F(P) = 0$ para todo ponto P de V.

Definição 2.1.11. *Um conjunto algébrico $V \subset \mathbb{P}^n$ é irredutível se não pode ser expresso como a união de dois subconjuntos algébricos próprios. Uma variedade algébrica projetiva é um conjunto algébrico irredutível em $\mathbb{P}^n$.*

Como no caso afim, temos o seguinte resultado.

Proposição 2.1.12. *Um conjunto algébrico projetivo V é irredutível se, e somente se, $I(V)$ é um ideal homogêneo primo.*

Seja $V \subset \mathbb{P}^n$ uma variedade projetiva, então o anel

$$A[V] = k[x_0, ..., x_n]/I(V)$$

é um domínio, chamado *anel de coordenadas homogêneas* de V. Note que, diferentemente do caso afim, um elemento de $A[V]$ não pode ser considerada uma função em V, a menos que sejam constante. Temos que $\bar{f} \in A[V]$ define uma função em V se e somente se $f(\lambda x_0, ..., \lambda x_n) =$

$f(x_0, ..., x_n)$ para todo $\lambda \in k^*$. Como $f = f_0 + ... + f_d$, onde cada f_i, $0 \leq i \leq d$, é um polinômio homogêneo de grau i, então isso acontece se e somente se

$$f(x_0, ..., x_n) = f(\lambda x_0, ..., \lambda x_n) = f_0(x_0, ..., x_n) + \lambda f_1(x_0, ..., x_n) + ... + \lambda^d f_d(x_0, ..., x_n)$$

para todo $\lambda \in k^*$, o que acontece somente no caso em que f é constante em V, logo, $\bar{f}$ é constante em $A[V]$. Sejam $\bar{f}, \bar{g}$ dois elementos de $A[V]$, $\bar{g} \neq 0$. Para o quociente $\bar{f}/\bar{g}$ fazer sentido é necessário que tais polinômios tenham o mesmo grau, pois nesse caso,

$$\frac{\bar{f}(\lambda a_0, \lambda a_1, ..., \lambda a_n)}{\bar{g}(\lambda a_0, \lambda a_1, ..., \lambda a_n)} = \frac{\lambda^{\partial f}\bar{f}(a_0, a_1, ..., a_n)}{\lambda^{\partial g}\bar{g}(a_0, a_1, ..., a_n)} = \frac{\bar{f}(a_0, a_1, ..., a_n)}{\bar{g}(a_0, a_1, ..., a_n)} \Longleftrightarrow \partial f = \partial g.$$

Dessa forma, podemos definir o corpo de frações de $A[V]$,

$$k(V) = \Big\{ \frac{\bar{f}}{\bar{g}} / \ \bar{f}, \ \bar{g} \ \in \ A[V] \text{ polinômios homogêneos de mesmo grau com } \bar{g} \neq 0 \Big\}.$$

Seja $V \subset \mathbb{P}^n$ uma variedade projetiva. Então o conjunto $V \cap \mathbb{A}^n = \varphi_i^{-1}(V \cap U_i)$ é uma variedade afim cujo ideal correspondente é dado por

$$I(V \cap \mathbb{A}^n) = \{f(x_0, ..., x_{i-1}, 1, x_{i+1}..., x_n) / f(x_0, ..., x_n) \in I(V)\}.$$

Como $\mathbb{P}^n = \cup_{i=0}^n U_i$, então V pode ser expressa como união de $n+1$ variedades afins $V = \cup_{i=0}^n V \cap U_i$.

Proposição 2.1.13. *Seja $V \subset \mathbb{P}^n$ uma variedade projetiva. Então*

$$k(V) \simeq k(V \cap U_i) \text{ para todo } i, \ 0 \leq i \leq n.$$

Demonstração. Defina a aplicação $\Phi \colon k(V) \longrightarrow k(V \cap U_i)$ por

$$\Phi\Big(\frac{\bar{f}}{\bar{g}}\Big) = \frac{\bar{f}(x_0, ..., 1, ..., x_n)}{\bar{g}(x_0, ..., 1, ..., x_n)}.$$

É fácil ver que Φ é uma bijeção cuja inversa é dada pela aplicação $\Gamma \colon K(V \cap U_i) \longrightarrow k(V)$ definida por

$$\Gamma\Big(\frac{\bar{h}}{\bar{l}}\Big) = \frac{x_i^d \bar{h}(x_0/x_i, ..., x_n/x_i)}{x_i^d \bar{l}(x_0/x_i, ..., x_n/x_i)}.$$

□

Dessa forma as propriedades locais de V podem ser completamente descritas em termos de suas partes afins $V \cap U_i$, esse é o caso por exemplo da dimensão.

Definição 2.1.14. *Seja $V \subset \mathbb{P}^n$ uma variedade projetiva. A dimensão de V é definida como $dim\ V :=$ grau de transcedência da extensão $k(V)/k$.*

Consequentemente, $dim\ V = dim\ (V \cap U_i)$. Em particular, $dim\ \mathbb{P}^n = dim\ \mathbb{A}^n = n$. O processo de substituir o polinômio $f(x_0, ..., x_n)$ pelo polinômio $f(x_1, ..., x_{i-1}, 1, x_{i+1}, ..., x_n)$, é chamado de *desomogeneização com respeito a* x_i. Esse processo pode ser revertido: dado um polinômio $f \in k[x_0, ..., x_n]$ de grau d, definimos a *homogeneização de f com respeito a* x_i por

$$f^*(x_0, ..., x_n) = x_i^d f\Big(\frac{x_0}{x_i}, \frac{x_1}{x_i}, ..., \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, ..., \frac{x_n}{x_i}\Big).$$

Definição 2.1.15. *Dada uma variedade afim $V \subset \mathbb{A}^n$, o fecho projetivo de V, denotado por $\bar{V}$, é a variedade projetiva*

$$\bar{V} = \{P \in \mathbb{P}^n / f^*(P) = 0 \text{ para todo } f \in I(V)\}.$$

Os pontos de $\bar{V} \backslash V$ são chamados os pontos no infinito em $\bar{V}$.

Nosso interesse em particular, é estudar as variedades algébricas planas, que descreveremos na próxima seção.

2.1.3 Curvas algébricas planas

Seja f um polinômio não constante e irredutível no anel de polinômios em duas variáveis $k[x, y]$. No exemplo 2.1.3, definimos uma *curva algébrica plana* como sendo a variedade no plano afim

$$V(f) = \{(x, y) \in \mathbb{A}^2 / f(x, y) = 0\}.$$

Observamos que se um polinômio $g \in k[x, y]$ é tal que $g = \lambda f,\ \lambda \in k^*$, então eles definem a mesma curva plana em $\mathbb{A}^2$. Dessa forma dois polinômios irredutíveis definem a mesma curva plana se, e somente se, eles diferem por um múltiplo constante não nulo. Isto nos motiva a fazer a seguinte definição.

Definição 2.1.16. *Uma curva algébrica plana afim é uma classe de equivalência do conjunto dos polinômios não constantes em $k[x, y]$, módulo a relação definida por*

$$f \sim g \text{ se, e somente se, existe } \lambda \in k^* \text{ tal que } f = \lambda g.$$

A equação de uma curva é qualquer um dos polinômios da classe de equivalência que a define. Nos referimos por C_f a curva plana afim definida por um polinômio f em $k[x, y]$. O

grau de uma curva C_f é o grau do polinômio f que a define, denotado por ∂f. Se $\partial f = 1$, então C_f é uma reta em $\mathbb{A}^2$, se $\partial f = 2$, C_f representa uma cônica em $\mathbb{A}^2$, se $\partial f = 3$, C_f representa uma uma cúbica em $\mathbb{A}^2$. Estamos interessados em estudar uma classe particular das curvas planas: as chamadas curvas planas *não singulares*.

Definição 2.1.17. *Seja C_f uma curva plana afim e $P = (a, b)$ um ponto em C_f. Se pelo menos uma das derivadas $\frac{\partial f}{\partial x}(P)$, $\frac{\partial f}{\partial y}(P)$ for diferente de zero, então P é um ponto não singular em C_f, caso contrário, P é um ponto singular de C_f.*

Dizemos que a curva plana C_f é não singular, se todos os seus pontos são não singulares. Como vimos anteriormente, dada uma curva plana afim, é sempre possível transformá-la em uma curva projetiva. O *fecho projetivo* de uma curva plana afim C_f é o subconjunto $\bar{C_f} \in \mathbb{P}^2$ formado pelas raízes do polinômio homogêneo

$$f^*(x, y, z) = z^{\partial f} f\Big(\frac{x}{z},\ \frac{y}{z}\Big);\ \bar{C_f} = \{(a : b : c) \in \mathbb{P}^2 / f^*(a, b, c) = 0\}.$$

Definição 2.1.18. *Uma curva plana projetiva é uma classe de equivalência de polinômios homogêneos não constantes em $k[x, y, z]$ módulo a relação $F \sim G \Leftrightarrow\ \exists\ \lambda \in k^*$ tal que $F = \lambda G$. Dado um polinômio homogêneo $F \in k[x, y, z]\backslash k$, denotamos por C_F a sua classe módulo a relação de equivalência $\sim$. O grau da curva C_F é o grau do polinômio F.*

Seja C_F a curva plana projetiva definida por $F(x, y, z) \in k[x, y, z]$. Temos que a curva C_F apresenta diversas partes afins, pois para cada escolha de plano obtemos uma curva plana afim C_f diferente: basta eliminar uma das variáveis x, y ou z utilizando uma das equações $x = 1$ ou $y = 1$, ou $z = 1$. Dessa forma a noção de singularidade e os demais conceitos introduzidos para curvas planas afins seguem naturalmente para curvas planas projetivas.

2.2 Interseções de curvas algébricas planas

Um dos problemas clássicos na teoria de curvas algébricas planas é calcular o número de pontos na interseção de duas curvas. O teorema de Bezout fornece explicitamente o número de pontos nessa interseção. Trataremos inicialmente do caso particular onde uma dessas curvas é uma reta.

2.2.1 Interseção de uma curva com uma reta

Sejam f um polinômio não constante em $k[x, y]$, C_f a curva plana afim definida por f e a reta l de equação $y = ax + b$. Um ponto $P = (x, y)$ pertence ao conjunto $C_f \cap l$ se suas coordenadas satisfazem a equação

$$f_l(x) := f(x, ax + b) = 0.$$

Temos as seguintes possibilidades para os pontos em $C_f \cap l$:

1. $f_l(x) = 0$, então $l \subset C_f$.

2. $f_l(x) = c \neq 0$, então $C_f \cap l = \emptyset$.

3. $f_l(x) = c\prod_{i=1}^{r}(x - x_i)^{m_i}$, onde c é uma constante não nula, r é o grau do polinômio f e x_i são as abscissas (duas a duas distintas) dos pontos de interseção $P_i = (x_i, ax_i + b)$.

Definição 2.2.1. *a multiplicidade ou índice de interseção das curvas l e C_f em um ponto P é dada por*

$$(l, C_f)_P = \begin{cases} 0, & se\ P \notin l \cap C_f \\ \infty, & se\ P\ \in l \subset C_f \\ m_i & se\ P = (x_i, ax_i + b)\ definido\ no\ caso\ 3\ acima. \end{cases}$$

Se l não é uma componente de C_f, definimos o inteiro

$$m_\infty := \partial f - \sum_{i=1}^{r} m_i$$

como a multiplicidade de interseção de l e C_f no infinito.

Exemplo 2.2.2. *Seja C_f a curva definida por*

$f(x, y) = y^2 - x^3 - x^2$ *e considere as retas $l_\pm$ definidas pelas equações $y = \pm x$. Temos que $f_{l_\pm} = x^2 - x^3 - x^2 = -x^3$, logo $O = (0, 0)$ é o único ponto em $C_f \cap l$, com multiplicidade $(l, f)_O = 3$.*

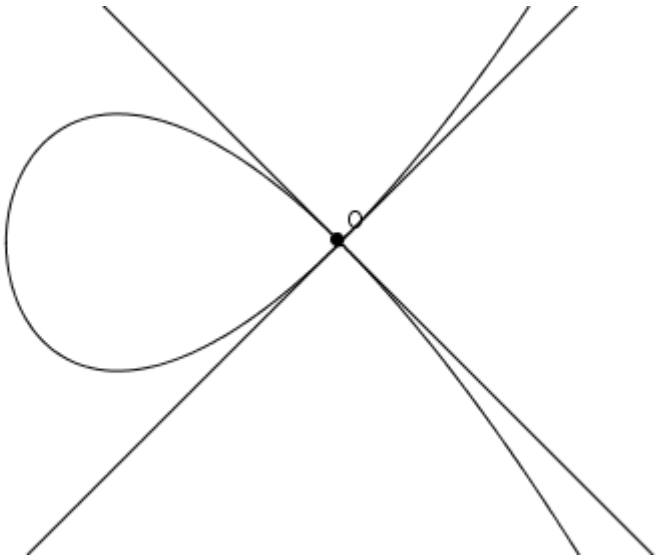

Figura 2.1: Multiplicidades de interseção $l_{\pm} \cap C_f$ na origem

Exemplo 2.2.3. *Sejam C_f e l as curvas definidas respectivamente pelos polinômios $f(x,y) = y - x^2$, $g(x,y) = ay + bx + c$. Então os pontos em $C_f \cap l$ são os pontos cujas coordenadas (x,y) satisfazem*

$$\begin{cases} y = x^2 \\ ax^2 + bx + c = 0 \end{cases}$$

Assim, $C_f \cap l$ consiste de dois pontos P e Q, a menos que $b^2 - 4ac = 0$ ou $a = 0$. Se $b^2 - 4ac = 0$, então a reta l é tangente a C_f, assim temos que C_f e l se intersectam em um único ponto R com multiplicidade 2. Se $a = 0$, então l é uma reta vertical, assim C_f e l se intersectam em um único ponto no plano afim, de multiplicidade 1. Nesse caso, temos $m_\infty = 1$. Veremos mais adiante, que se tomarmos os fechos projetivos de tais curvas, então o conjunto $\bar{C}_f \cap \bar{l}$ possui exatamente 2 pontos, contados com suas multiplicidades.

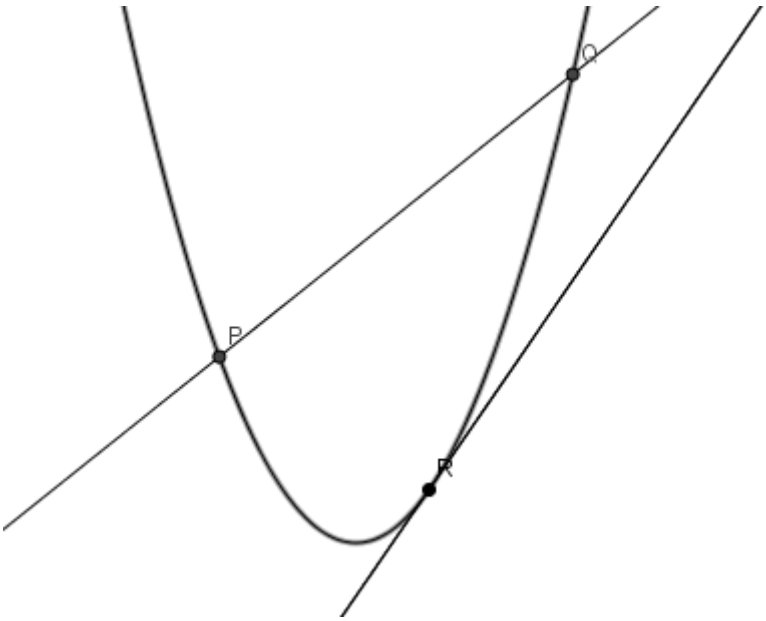

Figura 2.2: Multplicidades da interseção $C_f \cap l$ dos pontos P, Q e R

Nosso objetivo agora é definir o conceito de *multiplicidade de um ponto* em uma curva plana C_f arbitrária. Esse conceito vai nos permitir classificar se uma tal curva é singular ou não.

Proposição 2.2.4. *Sejam $f(x, y) \in k[x, y]$, C_f a curva definida por f e P um ponto em C_f. Existe um inteiro $m = m_P(C_f) \geq 1$ tal que, para toda reta l passando por P, temos*

$$(l, C_f)_P \geq m,$$

ocorrendo a desigualdade estrita para no máximo m retas e no mínimo uma.

Demonstração. Podemos supor, sem perda de generalidade que $P = (0, 0)$. Escrevamos

$$f = f_m + ... + f_d,$$

com f_i homogêneo de grau i, $m \leq i \leq d$ e $f_m \neq 0$. Se $P \in C_f$, temos que $m \geq 1$. Seja l_t a reta de equação $y - tx = 0$. Temos que

$$f_{l_t} = x^m \Big(f_m(1, t) + f_{m+1}(1, t)x + ... + f_d(1, t)x^{d-m} \Big)$$

Consequentemente, $(l_t, C_f)_P \geq m$, e a igualdade ocorre se e somente se, $f_m(1, t) \neq 0$. Como $f_m(1, t)$ é um polinômio em t de grau $m \geq 1$, ele se anula em no mínimo um e no máximo m valores de t distintos.

□

Definimos o inteiro $m = m_P(C_f)$ descrito na proposição acima como sendo a *multiplicidade do ponto* P na curva C_f. Se $P \notin C_f$, então $m_P(C_f) = 0$. Se $P = (x_0, y_0) \in C_f$, podemos decompor o polinômio homogêneo $f_m(x, y)$ de maneira única

$$f_m(x, y) = \prod (a_i x + b_i y)^{e_i}$$

tal que os fatores lineares $a_i x + b_i y$ são retas distintas. As retas

$$l_i = a_i(x - x_0) + b_i(y - y_0)$$

são as retas tangentes a C_f em P. O expoente e_i é a multiplicidade da tangente l_i. Voltando ao exemplo 2.2.2, observamos que $(l, C_F)_O = 3$ e $m_O(C_f) = 2$, isso $((l, C_f)_P > m_p(C_f))$ geralmente ocorre quando l é uma das retas tangentes à curva C_f no ponto P. Um ponto $P = (x_0, y_0) \in C_f$ é não singular ou que C_f é não singular em P, se $m_P(C_f) = 1$. Nesse caso, a *única* reta tangente à curva C_f em P tem equação

$$\frac{\partial f}{\partial x}(x_0, y_0)(x - x_0) + \frac{\partial f}{\partial y}(x_0, y_0)(y - y_0) = 0.$$

2.2.2 Interseção entre duas curvas planas

Proposição 2.2.5. *A interseção de duas curvas planas afins, sem componentes em comum, é finita.*

Demonstração. Sejam C_f e C_g as curvas planas afins definidas respectivamente pelos polinômios $f,\ g \in k[x, y]$. Sem perda de generalidade, podemos supor que f, g são polinômios em $k[x][y]\backslash k$, tais que $(f, g) = 1$. Pelo lema de Gauss, temos que $(f, g) = 1$ no anel $k(x)[y]$. Como $k(x)[y]$ é um domínio principal, assim existem elementos $\alpha, \beta \in k(x)[y]$ tais que $\alpha f + \beta g = 1$. Logo, existem polinômios $a, b \in k[x, y]$ e c em $k[x]\backslash\{0\}$ tais que $af + bg = c(x)$. Se $P = (x_0, y_0) \in C_f \cap C_g$, então $c(x_0) = 0$, e logo, existem finitas possibilidades para x_0. Fixado x_0, existe um número finito de possibilidades para y_0 tais que $f(x_0, y_0) = 0$. □

Os resultados acima descritos podem ser estendidos de forma natural para o caso projetivo. Em particular, se L é uma reta e C_F uma curva em $\mathbb{P}^2$, tais que $\mathcal{O} = (0 : 1 : 0) \in L \cap C_F$, então a multiplicidade de interseção $(L, C_F)_{\mathcal{O}}$ coincide com a multiplicidade m_∞ já definida anteriormente. A próxima questão natural é determinar o número de pontos na interseção $C_f \cap C_g$. Se C_f e C_g são curvas planas afins, conseguimos determinar apenas uma cota para $\#C_f \cap C_g$, pois os pontos no infinito não serão contados. Assim, tomando os polinômios $F = f^*$ e $G = g^*$, vamos considerar as curvas planas projetivas C_F e C_G.

Teorema 2.2.6 (Bezout)**.** *Sejam C_F e C_G curvas planas projetivas sem componentes irredutíveis em comum, tais que $\partial F = m$ e $\partial G = n$. Então o conjunto $C_F \cap C_G$ possui exatamente mn pontos, contados com suas multiplicidades.*

Corolário 2.2.7. *Sejam C_F e C_G duas cúbicas projetivas sem componentes comuns. Então a interseção $C_G \cap C_F$ possui exatamente nove pontos, contados com suas multiplicidades.*

Teorema 2.2.8. *Sejam C_F e C_G duas cúbicas projetivas sem componentes em comum e $A_1, ..., A_9$ os pontos na interseção $C_F \cap C_G$. Se uma cúbica C contém os pontos $A_1, ..., A_8$, então $A_9 \in C$.*

Demonstração. Sejam

$$H(x, y, z) = a_1x^3 + a_2x^2y + ... + a_{10}z^3,\ a_1, ..., a_{10} \in k$$

e C a cúbica definida por H. Os pontos $A_1 = (x_1 : y_1 : z_1), ..., A_8 = (x_8 : y_8 : z_8) \in C$ estão em posição geral se os vetores $(x_i^3, x_i^2y_i, ..., z_i^3)$ são linearmente independentes para todo i, $1 \leq i \leq 8$. Denote por Γ o conjunto formado pelas cúbicas que passam pelos pontos $A_1, ..., A_8$. Temos que Γ forma um espaço vetorial sobre k de dimensão 2. Assim podemos assumir que as cúbicas C_F e C_G formam uma base para Γ e logo, existem $\lambda,\ \mu \in k$ tais que

$$C = \lambda C_F + \mu C_G.$$

Consequentemente, $A_9 \in C$. O caso em que os pontos $A_1, ..., A_8$ não estão em posição geral, pode ser encontrado em [11], III, 6.2. □

2.3 Divisor de uma curva projetiva

Definição 2.3.1. *Seja C a curva projetiva definida pelo polinômio $F(x, y, z) \in k[x, y, z]$. Um divisor D da curva C, é a soma formal finita de pontos em C*

$$D = \sum_{P \in C} n_P(P),\ n_p \in \mathbb{Z}.$$

O grau de um divisor D é dado por

$$deg(D) = \sum_{P \in C} n_P.$$

O conjunto dos divisores de uma curva C sobre k, denotado por $\mathrm{Div}_k(C)$, é um grupo abeliano. Seja φ uma função racional não nula de C, isto é,

$$\varphi = \frac{G(x,y,z)}{H(x,y,z)},$$

onde $G,\ H$ são polinômios homogêneos de mesmo grau, digamos m, tal que F não divide H. A condição $\varphi \neq 0$ implica que F não divide G. Assim, pelo teorema de Bezout, temos

$$\partial(F).\ m = \sum_{P\ \in\ C\ \cap\ C_G} (C, C_G)_P$$
$$\partial(F).\ m = \sum_{P\ \in\ C\ \cap\ C_H} (C, C_H)_P$$

Defina o divisor de φ por

$$Div(\varphi) = \sum ord_P(\varphi)(P),\ \text{onde}$$
$$ord_P(\varphi) = \sum_{P\ \in\ C\ \cap\ C_G} (C, C_G)_P - \sum_{P\ \in\ C\ \cap\ C_H} (C, C_H)_P.$$

Note que, como G e H possuem o mesmo grau, temos que $deg(\varphi) = 0$. Um divisor de uma função racional em C é chamado de *principal*. Dois divisores D_1 e D_2 são *linearmente equivalentes*, $D_1 \sim D_2$ se $D_1 - D_2$ é um divisor principal. O conjunto dos divisores (φ) formam um subgrupo $P(C)$, chamado subgrupo dos *divisores principais*. Denotando por $Div^0(C)$ o grupo dos divisores de grau zero, segue que $P(C) \subset Div^0(C)$. Dessa forma, faz sentido considerar o quociente do grupo $\mathrm{Div}_k(C)$ por $P(C)$, a saber, os chamados *grupos de Picard* ou *grupo das classes* de um divisor de C,

$$Pic(C) = \frac{\{D\backslash\ D \in Div_k(C)\}}{\{(\varphi)\backslash\ \varphi \in k^*\}}\ ;\ Pic^0(C) = \frac{\{D\backslash\ D \in Div_k^0(C)\}}{\{(\varphi)\backslash\ \varphi \in k^*\}}\ .$$

Veremos no próximo capítulo que quando C é uma *curva elíptica* definida sobre o corpo k, a estrutura do grupo $Pic^0(C)$ induz uma estrutura de grupo sobre C.

Definição 2.3.2. *Dado um divisor $D \in Div(C)$, associamos o conjunto de funções*

$$\mathcal{L}(D) = \{\varphi \in k(C)/\ div(\varphi) + D \geq 0\} \cup \{0\}.$$

O conjunto $\mathcal{L}(D)$ é um espaço vetorial sobre k de dimensão finita, denotada por

$$l(D) = dim_k \mathcal{L}(D).$$

Note que se um divisor D é tal que $deg(D) < 0$, então $\mathcal{L}(D) = \{0\}$ e $l(D) = 0$, pois se $\varphi \in \mathcal{L}(D)\backslash\{0\}$ então

$$0 = deg\ div(\varphi) \geq deg(-D) = -deg(D).$$

Assim, devemos ter $deg(D) \geq 0$. O próximo teorema é um resultado fundamental na teoria de curvas algébricas.

Teorema 2.3.3 (Riemann)**.** *Seja C uma curva projetiva não singular. Existe um inteiro $g \geq 0$, chamado o gênero de C, tal que para todo divisor $D \in Div(C)$,*

$$l(D) \geq deg(D) + 1 - g,$$

Demonstração. Ver [9], página 23. □

Em particular, quando C é uma curva plana projetiva não singular, definida pelo polinômio $F \in k[x, y, z]$, o gênero de C pode ser completamente determinado pelo grau do polinômio F, pela fórmula

$$g(C) = \frac{(\partial F - 1)(\partial F - 2)}{2}.$$

Assim, curvas planas projetivas não singulares de grau 1 ou 2 possuem gênero $g = 0$, curvas de grau 3 ou 4 não singulares possuem gênero $g = 1$. Em particular, uma curva elíptica, cuja teoria será fundamental na compreensão do nosso objeto de estudo, é uma curva plana projetiva de gênero um, com algum ponto racional .

Capítulo 3

Curvas Elípticas

Curvas elípticas terão um papel de destaque na compreensão do nosso objeto de estudo. Tais curvas são particularmente interessantes por apresentarem uma rica estrutura aritmética: o conjunto dos pontos racionais de uma curva elíptica E admite uma estrutura de grupo abeliano. Nosso foco nesse capítulo é estudar a estrutura desse grupo que, como veremos, é um grupo abeliano finitamente gerado. Demonstrações de teoremas e proposições aqui mencionados podem ser encontradas em [8] e [7].

3.1 Forma de Weierstrass de uma curva elíptica

Definição 3.1.1. *Uma curva elíptica E definida sobre um corpo k, é uma curva plana projetiva não singular de equação*

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \tag{3.1}$$

onde $a_1, ..., \ a_6 \in k$.

O único ponto no infinito é dado por $\mathcal{O} = (0 : 1 : 0)$, obtido fazendo $Z = 0$ na equação acima. A equação (3.1) é chamada *forma de Weierstrass* de uma curva elíptica.

Usando coordenadas não homogêneas $x = X/Z$ e $y = Y/Z$, a curva elíptica E na forma de Weierstrass é dada por

$$E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{3.2}$$

Quando o corpo k possui característica diferente de 2 e 3, a mudança de variáveis

$$x' = x, \ y' = y + \frac{a_1}{2}x,$$

elimina o termo xy em (3.1), e a mudança de variáveis

$$x' = x + \frac{a_2}{3},\ y' = y + \frac{a_3}{2},$$

elimina os termos x^2 e y. Assim, assumindo que a característica de k é diferente de 2 e 3, a forma de Weierstrass de uma curva elíptica E definida sobre k é

$$E\colon y^2 = x^3 + ax + b. \tag{3.3}$$

Proposição 3.1.2. *Seja k um corpo de característica diferente de 2 e 3. Então toda curva elíptica sobre k é isomorfa a uma curva da forma*

$$E\colon y^2 = x^3 + ax + b,\ a, b \in k.$$

A curva E é não singular, se e somente se, o discriminante da forma de Weierstrass $\Delta = -16(4a^3 + 27b^2)$ é diferente de zero.

Demonstração. O ponto $(0 : 1 : 0)$ é não singular, pois

$$\frac{\partial F}{\partial Z}(0 : 1 : 0) = 1,\ F = f^*.$$

O polinômio $f(x) = x^3 + ax + b$ possui raízes múltiplas, se e somente se a resultante de f e f', que é o determinante de uma matriz específica formada pelos coeficientes de f e f', for diferente de zero, o que ocorre quando $4a^3 + 27b^2 \neq 0$. □

Mais geralmente, se $y^2 = f(x)$ onde f é um polinômio de grau três ou quatro sem raízes múltiplas, então tal equação define uma curva plana não singular de gênero um, e portanto uma curva elíptica no plano afim. A interseção de duas superfícies quadráticas, no espaço projetivo tridimensional, também descreve uma curva elíptica, desde que tenha pelo menos um ponto racional. Veremos na próxima seção que o conjunto dos pontos de uma curva elíptica admite estrutura de um grupo abeliano, com elemento neutro como sendo o ponto $\mathcal{O} = (0 : 1 : 0)$.

3.2 Operação entre os pontos de uma curva elíptica

Usaremos a notação $E(k)$ para o conjunto de pontos no plano projetivo situados na curva elíptica E,

$$E(k) = \{(x,\ y) \in \mathbb{A}^2_k;\ y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}.$$

Sejam P e Q pontos em $E(k)$, então o teorema de Bezout garante a existência de um terceiro ponto R em $E(k)$, como sendo a interseção da curva com a reta que passa pelos pontos P e Q. Se a reta é tangente à curva em um ponto, esse ponto terá multiplicidade dois; se a reta é paralela ao eixo y, definimos o terceiro ponto como sendo o ponto no infinito. Dessa forma é possível definir uma operação entre os pontos de $E(k)$ da seguinte maneira.

A lei de Grupo

- Sejam P e Q pontos de $E(k)$;
- Seja r a reta passando pelos pontos P e Q e seja $P * Q$ o terceiro ponto de interseção da curva $E(k)$ com a reta r;
- Repetindo-se o processo com os pontos $P * Q$ e $\mathcal{O}$, o terceiro ponto obtido nesse processo será a soma $P + Q$.
- se $P = Q$, tomamos a reta tangente à curva neste ponto.

Proposição 3.2.1. *A operação acima tem as seguintes propriedades:*

(*a*) *(Existência do elemento neutro)* $P + \mathcal{O} = P$ *para todo* $P \in E(k)$.

(*b*) *(Comutatividade)* $P + Q = Q + P$ *para todo* $P, Q \in E(k)$.

(*c*) *(Existência do elemento inverso) Seja* $P \in E(k)$. *Então existe um ponto de* $E(k)$, *denotado por* $-P$, *satisfazendo*

$P + (-P) = \mathcal{O}$.

(*d*) *(Associatividade) Sejam* $P,\ Q,\ R \in E(k)$. *Então* $(P + Q) + R = P + (Q + R)$.

Demonstração. Vamos mostrar que $E(k)$ admite estrutura de grupo abeliano, com elemento neutro $\mathcal{O}$. Pelo teorema de Bezout, a operação está bem definida.

(*a*) Seja $P = (x_1, y_1) \in E(k) \backslash \{\mathcal{O}\}$. Para calcular o ponto $P + \mathcal{O}$, tomemos a reta que passa por P e por $\mathcal{O}$, neste caso, a reta vertical passando por P. O terceiro ponto de interseção será o ponto de coordenadas $(x_1,\ -y_1)$. Assim, $P + \mathcal{O} = P$, para todo ponto $P \in E(k)$, e logo, o ponto $\mathcal{O}$ é o elemento neutro da operação.

(*b*) Pela definição, é fácil ver que a operação é comutativa.

(*c*) Sejam $P = (x_1, y_1),\ -P = (x_1, -y_1)$ e l a reta passando por P e $-P$. Então $P*(-P) = \mathcal{O}$ e logo $P + (-P) = \mathcal{O}$.

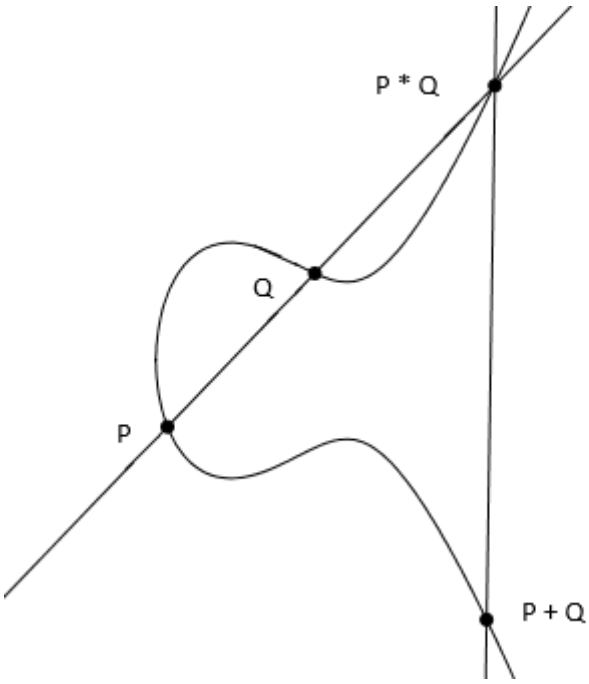

Figura 3.1: Adição de pontos em uma curva elíptica

(d) Dados dois pontos P e Q denote por $l(P,Q)$ a reta em $\mathbb{P}^2$ passando por P e Q. Sejam $P,\ Q$ e $R \in E(k)$. Para mostrar que $(P+Q)+R = P+(Q+R)$, é suficiente mostrar que $(P+Q)*R = P*(Q+R)$. Seja S o ponto de interseção das retas $l(P,Q+R)$ e $l(R,P+Q)$. Vamos mostrar que $S \in E(k)$. Considere a cúbica E_1 formada pela união das retas $l(P,Q),\ l(R,P+Q),\ l(Q*R,\mathcal{O})$ e E_2 formada pela união das retas $l(P,Q*R),\ l(Q,R),\ l(P,\mathcal{O})$ Então

$$E_1 \cap E_2 = \{\mathcal{O}, P, Q, R, P*Q, Q*R, P+Q, Q+R, S\}$$

Temos que $E(k)$ passa pelos oito pontos $\mathcal{O}, P, Q, R, P*Q, Q*R, P+Q, Q+R$, e logo pelo teorema 2.2.8 segue que $S \in E(k)$. □

Sejam $P_1 = (x_1,\ y_1),\ P_2 = (x_2,\ y_2)$ pontos de $E(k)\backslash\{\mathcal{O}\}$, as fórmulas explicitas para obter as coordenadas do ponto $P_1 + P_2$ podem ser encontradas em [8], página 53.

Um dos resultados mais importantes sobre a estrutura do grupo $E(k)$ é dado pelo seguinte teorema.

Teorema 3.2.2 (Mordell - Weil)**.** *O grupo dos pontos racionais de uma curva elíptica é um grupo abeliano finitamente gerado,*

$$E(k) \cong E(k)_{tor} \oplus \mathbb{Z}^r$$

onde $E(k)_{tor}$ é o subgrupo dos elementos de ordem finita, chamado grupo de torção e r é chamado posto de $E(k)$.

Isto significa que existe um conjunto finito $\{P_1, P_2, ..., P_s\},\ s > r$, de pontos de $E(k)$ tal que todo elemento de $E(k)$ é da forma $n_1P_1 + n_2P_2 + ... + n_sP_s$ com $n_1, ..., n_s \in \mathbb{Z}$. Tendo definido a estrutura geral de um grupo formado por pontos de uma curva elíptica, uma questão que naturalmente surge é a quantidade de elementos de tal grupo. Para o grupo de torção, temos um importante resultado que determina todas as possibilidades para $E(k)_{tor}$, em particular estabelece que a quantidade de elementos de ordem finita em $E(k)$ é no máximo 16.

Teorema 3.2.3 (Mazur)**.** *Se $E(k)_{tor}$ não for trivial, então é isomorfo a um dos* 14 *grupos:*

1. $\mathbb{Z}_n,\ 1 \leq n \leq 10$ *ou* $n = 12$.

2. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}, 1 \leq n \leq 4$.

Em particular, $\#E(k)_{tor} \leq 16$.

Note que, segundo este teorema, a ordem dos pontos de $E(k)_{tor}$ é no máximo 12 e não existem pontos de ordem 11. O próximo resultado estabelece uma maneira para determinar os elementos de ordem finita em $E(k)$.

Teorema 3.2.4 (Nagell - Lutz)**.** *Sejam E a curva elíptica sobre k definida pela equação $y^2 = x^3 + ax + b$, com $a, b \in \mathbb{Z}$. Então as coordenadas de um ponto $P = (x_0, y_0) \in E(k)_{tor}$ são números inteiros. Além disso, P tem ordem 2 ou $y_0^2 |\ \Delta$, onde $\Delta = -16(4a^3 + 27b^2)$.*

Os pontos (x_0, y_0) de ordem 2 em $E(k)_{tor}$ são exatamente os que tem a coordenada y_0 igual a zero, pois nesse caso,

$$2P = \mathcal{O} \iff P = -P \iff y_0 = -y_0.$$

A estrutura do grupo $\mathrm{Pic}^0(E)$ definido no capítulo anterior, induz uma estrutura de grupo em $E(k)$, que é a mesma que definimos anteriormente. Isto pode ser esclarecido a partir da seguinte proposição.

Proposição 3.2.5. *Sejam E uma curva elíptica definida sobre k e $\mathcal{O} \in E(k)$. Então a aplicação*

$$\begin{aligned} \Phi\colon E(k) &\longrightarrow Pic_k^0(E) \\ P &\longmapsto [P] - [\mathcal{O}] \end{aligned}$$

é uma bijeção.

Demonstração. Ver [7], página 35. □

A bijeção $E(k) \longrightarrow Pic_k^0(E)$ define uma estrutura de grupo abeliano em $E(k)$, que é determinada pela condição: $P + Q = S$ se e somente se $[P] + [Q] \sim [S] + [\mathcal{O}]$. Sejam P, Q, R, S pontos em $E(k)$ tais que $P * Q = R$ e $P + Q = S$. Sejam l_1 a reta intersectando E nos pontos P, Q e R e l_2 a reta intersectando E em R, S e $\mathcal{O}$. As retas l_1, l_2 podem ser consideradas como sendo polinômios homogêneos de grau um. Considere a função racional $h = \frac{l_1}{l_2} \in k(E)$, então h possui zeros nos zeros de l_1 e polos no zeros de l_2. Assim o divisor de h em E é $(h) = [P] + [Q] + [R] - [\mathcal{O}] - [R] - [S] = [P] + [Q] - [S] - [\mathcal{O}]$,. Portanto, temos que $[P] + [Q] \sim [S] + [\mathcal{O}]$ e $P + Q = S$.

Capítulo 4

Contraexemplo para a Conjectura no caso $n = 4$

4.1 Considerações Iniciais

O conhecido Teorema de Fermat afirma que para qualquer expoente $n \geq 3$ não existem soluções no conjunto dos números inteiros positivos para a equação $x^n + y^n = z^n$. Diversos matemáticos tentaram demonstrar tal teorema, em particular, Euler ficou especialmente interessado nas descobertas de Fermat, dando uma prova para o caso $n = 3$. Ele provou que a soma de cubos não nulos não poderia resultar em um cubo, mas ele também observou que a soma de três cubos não nulos poderia resultar em um cubo. A partir dessa observação, Euler propôs que para expoentes $n > 3$, a soma de k potências de números inteiros positivos com expoente n é igual a uma tal potência se $k \geq n$, caso contrário, essa soma não gera uma potência n - ésima. Em particular, ele estava convencido que a soma de três potências quárticas de números inteiros positivos não poderia resultar em uma tal potência, por outro lado, a equação $a^4 + b^4 + c^4 + d^4 = e^4$ teria soluções inteiras não triviais.

Em 1988 Noam Elkies, usando a teoria de curvas elípticas, obteve o seguinte contraexemplo para o caso $n = 4$:

$$2682440^4 + 15365639^4 + 18796760^4 = 20615673^4.$$

No presente capítulo, exibiremos o método encontrado por Elkies para encontrar o contraexemplo mencionado acima, destacando o papel da curva elíptica na descoberta de tal solução. Vamos buscar inicialmente pontos racionais (r, s, t) da superfície $S_1 \colon r^4 + s^4 + t^4 = 1$, que

também é equivalente a buscar pontos racionais da superfície $S_2\colon r^4 + s^4 + t^2 = 1$ com a condição adicional de t ser um quadrado. A vantagem de se trabalhar nesse ambiente é que a superfície S_2 pode ser parametrizada por uma família de cônicas, sendo possível reescrever a equação inicial na forma $ax^2 + by^2 + cz^2 = 0$. Os números inteiros positivos satisfazendo esta equação estão associados com os pontos racionais de uma curva elíptica E definida sobre $\mathbb{Q}$. Além disso, se um ponto em $E(\mathbb{Q})$ possui ordem infinita, então teremos uma infinidade de soluções inteiras não triviais para a equação diofantina estudada.

4.2 A superfície S_2

De acordo com [3], a superfície S_2 em $\mathbb{Q}^3$ determinada por

$$r^4 + s^4 + t^2 = 1, \tag{4.1}$$

pode ser parametrizada por uma família de cônicas U, a partir da aplicação

$$\begin{aligned} \phi\colon U &\longrightarrow S_2 \\ (x, y, u) &\longmapsto \left(x + y, x - y, \frac{4(u^2-2)x^2 + 8ux + (2-u^2)}{(u^2+2)}\right) \end{aligned}$$

onde a família de cônicas U é parametrizada por um parâmetro u da seguinte maneira:

$$r = x + y,\ s = x - y \tag{4.2}$$

$$(u^2 + 2)y^2 = -(3u^2 - 8u + 6)x^2 - 2(u^2 - 2)x - 2u \tag{4.3}$$

$$(u^2 + 2)t = 4(u^2 - 2)x^2 + 8ux + (2 - u^2). \tag{4.4}$$

Tal parametrização foi redescoberta, independentemente e de maneiras distintas, por Andrew Bremner, Don Zagier e Noam Elkies. Na abordagem de Bremner, a superfície S_2 foi expressa da seguinte forma:

$$2(1 + r^2)(1 + s^2) = (1 + r^2 + s^2)^2 + t^2.$$

considerando a fatoração de ambos os lados em $\mathbb{Q}[i]$. Já Zagier representou $1 - r^4 - s^4$ por meio de

$$1 - r^4 - s^4 = P_0^2 - 2Q_0R_0 \tag{4.5}$$

onde P_0 e Q_0 foram tomados a partir de casos especiais das cônicas 4.3 e 4.4, como os casos onde $u = 0$ e quando $u \to \infty$. As respectivas cônicas para estes casos são:

$$y^2 = -3x^2 - 2x; \quad t = 1 - 4x^2;$$
$$y^2 = -3x^2 - 2x; \quad t = 1 - 4x^2;$$
$$P_0 = 4x^2 - 1; \quad Q_0 = y + 3x^2 + 2x; \quad R_0 = y + 3x^2 - 2x.$$

Assim, temos uma infinidade de representações de $1 - r^4 - s^4$ como $P_0 - 2Q_0R_0$, em particular, quando $Q_0 = 0$ em (4.5), obtemos uma representação da superfície S_2.

De agora em diante, vamos trabalhar com as cônicas (4.3) e (4.4). Considerando a aplicação ϕ definida anteriormente, vamos mostrar que de fato, o conjunto $\phi(U)$ está contido em S_2, isto é, para todo $(x, y, u) \in U$, $f(\phi(x, y, u)) = 0$, onde $f(r, s, t) = r^4 + s^4 + t^2 - 1$ é o polinômio que define a superfície S_2. Segue da definição da aplicação ϕ que

$$\begin{aligned} f(\phi(x,y,u)) &= (x+y)^4 + (x-y)^4 + \Big(\frac{4(u^2-2)x^2 + 8ux + (2-u^2)}{(u^2+2)} \Big) - 1 \\ &= 2x^4 + 2y^4 + 12x^2y^2 + \frac{\sigma(x,u)}{(u^2+2)^2} - 1, \end{aligned}$$

onde $\sigma(x, u) =$

$$16u^4x^4 - 8x^2u^4 + u^4 - 64u^2x^4 + 48u^2x^2 - 4u^2 + 64x^4 - 32x^2 + 64u^3x^3 - 32u^3x - 128ux^3 + 32ux + 4.$$

Assim, $(u^2 + 2)f(\phi(x, y, u)) =$
$2(9x^4u^4 - 4u^4x^2 + 32u^3x^3 - 8u^3x - 28u^2x^4 + 48u^2x^2 - 4u^2 - 64ux^3 + 16ux + 36x^4 - 16x^2) +$
$12x^2y^2 + 2y^4$. Substituindo (4.3) temos então

$(u^2+2)^2 f(\phi(x,y,u)) = 18x^4u^4 - 8u^4x^2 + 64u^3x^3 - 16u^3x - 56u^2x^4 + 96u^2x^2 - 8x^2 - 128ux^3 +$
$31ux + 72x^4 - 32x^2 - 36u^4x^4 - 24u^4x^3 + 96u^3x^4 - 24u^3x^2 - 144u^2x^4 + 192ux^4 - 48ux^2 - 144x^4 +$
$96x^3 + 2(9u^4x^4 - 48u^3x^2 + 100u^2x^4 - 96ux^4 + 36x^4 + 12u^4x^3 - 32u^3x^3 + 12u^3x^2 - 32u^2x^2 +$
$64ux^3 + 24ux^2 - 48x^3 + 4u^4x^2 + 8u^3x - 16u^2x^2 + 4u^2 - 16ux + 16x^2) = 0$

A aplicação inversa para ϕ pode ser definida da seguinte forma

De (4.2) temos que $x = \dfrac{r+s}{2}$, $\quad y = \dfrac{r-s}{2}$. De (4.3) obtemos uma equação quadrática em u

$$(y^2 + 3x^2 + 2)u^2 + (2 - 8x)u + (2y^2 + 6x^2 - 2x) = 0 \tag{4.6}$$

com discriminante $\Delta = 4(1 - (2x^4 + 12x^2y^2 + 2y^4)$. Substituindo (4.2) e (4.3) temos

$$u = \frac{-1 + (r+s)^2 \pm t}{r^2 + rs + s^2 + r + s} \tag{4.7}$$

Daí, a aplicação

$$\psi(r,s,t) = \Big(\frac{r+s}{2} \, , \, \frac{r-s}{2} \, , \, \frac{-1+(r+s)^2+t}{r^2+rs+s^2+r+s} \Big)$$

é uma aplicação racional de S_2 definida nos pontos de S_2 que satisfazem $r^2+s^2+rs+r+s \neq 0$. De fato, vamos mostrar que para todo $(r,s,t) \in S_2$, temos $h(\psi(r,s,t)) = 0$ onde $h(x,y,u) = (u^2+2)y^2 + (3u^2-8u+6)x^2 + 2(u^2-2)x + 2u$.

Temos

$$h(\psi(r,s,t)) = \Big(\frac{-1+(r+s)^2+t}{r^2+rs+s^2+r+s} \Big)^2 \Big[\Big(\frac{r-s}{2} \Big)^2 + 3\Big(\frac{r+s}{2} \Big)^2 + 2\Big(\frac{r+s}{2} \Big) \Big]$$

$$+ \; 2\Big(\frac{r-s}{2} \Big)^2 + \Big(\frac{-1+(r+s)^2+t}{r^2+rs+s^2+r+s} \Big) \Big[-8\Big(\frac{r+s}{2} \Big)^2 + 2 \Big] + 6\Big(\frac{r+s}{2} \Big)^2 - 2(r+s)$$
$$= \frac{r^4+s^4+t^2-1}{r^2+s^2+rs+r+s} = 0.$$

Logo, todo ponto racional (r,s,t) em S_2 pertence a cônica (4.3), para algum valor racional de u.

Lema 4.2.1. *A aplicação*

$$\gamma(x,y,u) = \Big(-x, y, \frac{2}{u} \Big)$$

é uma involução em U, para $u \neq 0$.

Demonstração. Temos que para $u \neq 0$

$$\gamma \circ \gamma(x,y,u) = \gamma\Big(-x, y, \frac{2}{u} \Big) = \Big(-(-x), y, \frac{2}{\frac{2}{u}} \Big) = (x,y,u).$$

Vamos mostrar que $h(-x, y, \frac{2}{u}) = 0$, para $u \neq 0$, onde

$h(x,y,u) = (u^2+2)y^2 + (3u^2-8u+6)x^2 + 2(u^2-2)x + 2u$ e $h(x,y,u) = 0$ em U. Nestas condições,

$$h(-x,y,\frac{2}{u}) = \Big(\frac{4+2u^2}{u^2} \Big)y^2 + \Big(\Big(\frac{12}{u^2}\Big) - \Big(\frac{16}{u}\Big) + 6 \Big)x^2 + 2\Big(\frac{2u^2-4}{u^2} \Big)x + \frac{4}{u} = \frac{2}{u^2}h(x,y,u) = 0.$$

□

Para todo ponto (x,y,u) com $u \neq 0$, temos que o ponto $\phi \circ \gamma(x,y,u)$ está em S_2. A involução γ nos garante que para qualquer valor racional de u o ponto $\Big(x, y, \frac{2}{u}\Big)$ está em U, em particular, existem m, n inteiros relativamente primos, com n ímpar e $m \geq 0$ tais que $\Big(x, y, \frac{2m}{n}\Big)$ está em U. Reescrevendo as equações (4.3), (4.4) para $u = \frac{2m}{n}$, com m, n nas condições acima, temos respectivamente as equações

$$(2m^2 + n^2)y^2 = -(6m^2 - 8mn + 3n^2)x^2 - 2(2m^2 - n^2)x - 2mn \tag{4.8}$$

$$(2m^2 + n^2)t = 4(2m^2 - n^2)x^2 + 8mnx + (n^2 - 2m^2). \tag{4.9}$$

É fácil ver que os números $m, n, 2m^2 + n^2, 2m^2 \pm 2mn + n^2, 2m^2 \pm 4mn + n^2$ são dois a dois relativamente primos. Como n é ímpar, basta usar o fato que $(m, n) = 1$ e a propriedade $(k, l) = (k, l - qk)$, k, l inteiros não nulos relativamente primos. Queremos representar a equação (2.7) num modelo que já tenha um método de resolução conhecido, para isto, vamos precisar estudar alguns conceitos da teoria dos números, como a reciprocidade quadrática e o teorema de Legendre.

Definição 4.2.2. *Sejam a, m números inteiros não nulos com $(a, m) = 1$. Então a é um resíduo quadrático módulo m se existe solução da equação $a \equiv x^2\ mod(m)$.*

Por exemplo, 2 é um resíduo quadrático módulo 7, mas 3 não é, pois $2 \equiv 3^2\ mod(7)$ e $x^2 - 3 \neq 0$ em $\mathbb{Z}_7$.

Observação 4.2.3. *Daqui em diante vamos adotar a expressão $m\ R\ n$ para denotar que m é um resíduo quadrático módulo n.*

Definição 4.2.4. *Seja p um primo ímpar. O símbolo de Legendre é definido por*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{se } a\ R\ p; \\ 0, & \text{se } p \mid a; \\ -1, & \text{se } a \text{ não é resíduo quadrático módulo } p; \end{cases}$$

Por exemplo, temos $\left(\frac{2}{7}\right) = 1$ e $\left(\frac{3}{7}\right) = -1$. O símbolo de Legendre é um dispositivo bastante útil para discussão de resíduos quadráticos. Vamos utilizar algumas de suas propriedades:

Proposição 4.2.5. *Seja p um número inteiro primo ímpar.*

1. $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) mod(p)$
2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;
3. *Se* $a \equiv b\ mod(p)$, *então* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;

Demonstração. Se p divide a ou b, a prova é imediata. Assumimos que $p \nmid a$ e $p \nmid b$.

1. Temos que $a^{p-1} \equiv 1\ mod\ (p)$, assim, $(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv\ 0\ mod\ (p)$. Logo, $a^{\frac{p-1}{2}} \equiv\ \pm 1\ mod\ (p)$, ou seja, $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\ mod\ (p)$.

2. Temos que $(ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}}$. Pelo item 1 temos que $(ab)^{\frac{p-1}{2}} \equiv \left(\frac{ab}{p}\right)\ mod\ (p)$ e $a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, segue que $\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

3. Direto da definição.

□

O próximo resultado fornece uma caracterização dos primos p ímpares nos quais 2 é um resíduo quadrático módulo p.

Lema 4.2.6. *Seja p um número inteiro primo ímpar. Então $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$, isto é, 2 é um resíduo quadrático módulo primos da forma $8k \pm 1$.*

Demonstração. Seja ε uma raíz primitiva oitava da unidade e $\gamma = \varepsilon + \varepsilon^{-1}$. Temos que $\gamma^2 = \varepsilon^2 + 2\varepsilon\varepsilon^{-1} + \varepsilon^{-2} = 2$. Assim,

$$\gamma^{p-1} = (\gamma^2)^{\frac{p-1}{2}} = 2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) mod(p)\ \text{(propriedade 1)} \Longrightarrow \gamma^p \equiv \left(\frac{2}{p}\right)\gamma\ mod(p).$$

Desenvolvendo a expressão, temos

$$\gamma^p = (\varepsilon + \varepsilon^{-1})^p = \varepsilon^p + \binom{p}{1}\varepsilon^{p-1} + ... + \varepsilon^{-p} \Longrightarrow \gamma^p \equiv \varepsilon^p + \varepsilon^{-p}\ mod(p).$$

Como p é primo ímpar, temos dois casos a considerar:

1. $p = 8k \pm 1 \Longrightarrow \varepsilon^p + \varepsilon^{-p} = \varepsilon + \varepsilon^{-1} = \gamma$.

2. $p = 8k \pm 3 \Longrightarrow \varepsilon^p + \varepsilon_8^{-p} = -\varepsilon - \varepsilon^{-1} = -\gamma$. Logo, $\gamma^p \equiv \gamma\ mod(p)$, se $p = 8k \pm 1$ e $\gamma^p \equiv -\gamma\ mod(p)$, se $p = 8k \pm 3$. Assim,

$$\gamma^p \equiv (-1)^{\frac{p^2-1}{8}}\gamma\ mod(p) \Longrightarrow (-1)^{\frac{p^2-1}{8}} \equiv \left(\frac{2}{p}\right)\ mod(p).$$

□

Vamos reescrever a equação (2.7) na forma

$$aX^2 + bY^2 + cZ^2 = 0. \tag{4.10}$$

As condições necessárias e suficientes para que a equação acima tenha solução inteira não trivial são dadas pelo seguinte teorema.

Teorema 4.2.7 (Legendre)**.** *Sejam a, b e c números inteiros não nulos, livres de quadrados, dois a dois relativamente primos e nem todos de mesmo sinal. Então a equação (4.10) possui uma solução inteira não trivial se e somente se as seguintes condições são satisfeitas:*

$$\Big(-\frac{ab}{c}\Big) = \Big(-\frac{ac}{b}\Big) = \Big(-\frac{bc}{a}\Big)$$

Demonstração. Ver [5], pág. 272 . □

Queremos colocar a equação (4.8) no modelo da equação (4.10), para isto, precisamos definir duas funções que nos fornecerão os coeficientes da nova equação, nas hipóteses do Teorema de Legendre.

Definição 4.2.8. *Dado um inteiro $k \neq 0$, definimos*

a) $S(k)$ é o maior inteiro positivo cujo quadrado divide k;

b) $R(k) = \frac{k}{S(k)^2}$.

Por exemplo, tomando $k = 48 = 2^4.3$ temos $S(k) = 4$ e $R(k) = 3$. Em particular, se k for um primo qualquer, temos $S(k) = 1$ e $R(k) = k$.

Observação 4.2.9. *Note que o número $R(k)$ é um inteiro livre de quadrados.*

Observação 4.2.10. *Dados l, j inteiros não nulos, primos entre si, é fácil ver que $R(lj) = R(l)R(j)$.*

Lema 4.2.11. *A cônica (4.8) tem infinitas soluções racionais (x, y) se $R(2m^2+n^2)$ e $R(2m^2-4mn+n^2)$ são ambos produtos de primos congruentes a 1 módulo 8.*

Demonstração. Vamos colocar (4.8) na forma

$$aX^2 + bY^2 + cZ^2 = 0,$$

nas condições do teorema acima. Tomando $X = 2mn + (2m^2 - n^2)x$ em (4.8), temos:

$$(2mn + (2m^2 - n^2)x)^2 = 4m^2n^2 + 2(2mn)(2m^2 - n^2)x + (2m^2 - n^2)^2x^2 =$$

$$4m^2n^2 + (8m^3n - 4mn^3)x + (4m^4 - 4m^2n^2 + n^4)x^2 =$$

$$2mn[2mn + 2(2m^2 - n^2)x + (6m^2 - 8mn + 3n^2)x^2] + (4m^4 - 12m^3n + 12m^2n^2 - 6mn^3 + n^4)x^2$$

Substituindo (4.8) na expressão acima temos:

$$(2mn + (2m^2 - n^2)x)^2 = -2mn(2m^2 + n^2)y^2 + (2m^2 - 2mn + n^2)(2m^2 - 4mn + n^2)x^2 \quad (4.11)$$

Sejam $\alpha = S(2mn(2m^2+n^2))$ e $\beta = S((2m^2-2mn+n^2)(2m^2-4mn+n^2)$. Tomando $Y = \alpha y$ e $Z = \beta x$ temos que $a = 1, b = R(2mn(2m^2+n^2))$ e $c = R((2m^2-2mn+n^2)(2m^2-4mn+n^2)$ em (4.10), a equação (4.11) fica na forma

$$X^2 + bY^2 - cZ^2 = 0. \tag{4.12}$$

Note que

$$x = \frac{X}{2mn + (2m^2 - n^2)} = \frac{Z}{\beta} \; e \; y = \frac{Y}{\alpha}.$$

Assim, para cada solução não trivial da equação (4.12) conseguimos uma solução não trivial para a equação (4.8).

Pelo teorema anterior, a equação (4.12) possui solução racional se e somente se $-b$ e $-c$ são resíduos quadráticos módulo c e b respectivamente.

Devemos ter $-b \equiv w^2 mod(c) \Rightarrow -b.\alpha^2 \equiv (w.\alpha)^2 mod(c) \Rightarrow -2mn(2m^2+n^2) \equiv v^2 mod(c)$ Precisamos saber se $b = -2mn(2m^2+n^2)$ é um resíduo quadrático módulo $c = R(2m^2-2mn+n^2)R(2m^2-4mn+n^2)$. Pelo Teorema Chinês dos Restos, basta verificar que $-2mn(2m^2+n^2)$ é um resíduo quadrático módulo cada fator primo na fatoração de $R(2m^2-2mn+n^2)$ e $R(2m^2-4mn+n^2)$.

Da mesma forma, devemos ter $c \equiv k^2 mod(b) \Rightarrow c\beta^2 \equiv (k\beta)^2 mod(b) \Rightarrow (2m^2-2mn+n^2)(2m^2-4mn+n^2) \equiv p^2 mod(b)$.

Ou seja, $(2m^2-2mn+n^2)(2m^2-4mn+n^2)$ deve ser um resíduo quadrático módulo cada primo dividindo $b = R(2mn(2m^2+n^2)) = 2R(m)R(n)R(2m^2+n^2)$.

Três dessas condições sempre são satisfeitas:

- $(2m^2-2mn+n^2)(2m^2-4mn+n^2) \equiv n^4 mod(m)$;
- $(2m^2-2mn+n^2)(2m^2-4mn+n^2) \equiv 4m^4 mod(n)$;
- $-2mn(2m^2+n^2) \equiv (2m^2-n^2)^2 mod(2m^2-2mn+n^2)$;

Como para cada número inteiro k, temos que $R(k)$ divide k, então $-2mn(2m^2+n^2)$ é um resíduo quadrático módulo $R(2m^2-2mn+n^2)$ e $(2m^2-2mn+n^2)(2m^2-4mn+n^2)$ é um resíduo quadrático módulo $2R(m)$ e $R(n)$;

As duas condições restantes produzem as restrições do lema 4.2.11, pois

- $(2m^2-2mn+n^2)(2m^2-4mn+n^2) \equiv 2(2mn)^2 mod(2m^2+n^2)$;

- $-2mn(2m^2+n^2) \equiv -2(2mn)^2 mod(2m^2-4mn+n^2)$;

Para que $(2m^2-2mn+n^2)(2m^2-4mn+n^2)$ (e portanto $R((2m^2-2mn+n^2)(2m^2-4mn+n^2))$) seja um resíduo quadrático módulo cada fator primo de $R(2m^2+n^2)$, precisamos que 2 seja um resíduo quadrático módulo $R(2m^2+n^2)$. É necessário que -2 também seja um resíduo quadrático módulo $R(2m^2+n^2)$, pois $n^2 \equiv -2m^2 mod(2m^2+n^2)$.

Analogamente, para que $R(2m^2+n^2)$ seja um resíduo quadrático módulo $R(2m^2-4mn+n^2)$, devemos ter 2 e -2 resíduos quadráticos módulo $R(2m^2-4mn+n^2)$, pois

- $-2mn(2m^2+n^2) \equiv -2(2mn)^2 mod(2m^2-4mn+n^2)$;
- $n^2 \equiv 2(m-n)^2 mod(2m^2-4mn+n^2)$;

Como 2 e -2 deverão ser resíduos quadráticos módulo cada primo p_i na fatoração de $R(2m^2-4mn+n^2)$ e de $R(2m^2+n^2)$, temos pelo lema (4.2.6) que $p_i = 8k \pm 1$ e

$$\left(\frac{-2}{p_i}\right) = 1 \Rightarrow \left(\frac{-1}{p_i}\right)\left(\frac{2}{p_i}\right) = 1 \Rightarrow \left(\frac{-1}{p}\right) = 1.$$

Logo, pelo item 1 da proposição 4.2.5 temos que $\frac{p_i-1}{2} = 2k$ e logo $p_i = 4k+1$. Concluímos, dessas três condições, que cada primo p_i na fatoração de $R(2m^2-4mn+n^2)$ e $R(2m^2+n^2)$, é da forma $8k+1$.

□

Exemplo 4.2.12. *Tomando $u = 4$, temos $4 = \frac{2m}{n}$, onde $(m,n) = (2,1)$. Assim, $2m^2+n^2 = 9$ e $2m^2-4mn+n^2 = 1$ e logo $R(9) = 1 = R(1)$. Portanto $(m,n) = (2,1)$ satisfaz as hipóteses do Lema (4.2.11), assim na equação (4.8), obtemos uma cônica de equação*

$$C : 9y^2 = -11x^2 - 14x - 4. \tag{4.13}$$

O ponto $(x,y) = \left(\frac{-1}{2}, \frac{1}{6}\right)$ é uma solução racional dessa equação e portanto $(r,s,t) = \left(\frac{1}{3}, \frac{2}{3}, \frac{8}{9}\right)$ é uma solução para a equação (4.1). A partir do ponto $\left(\frac{-1}{2}, \frac{1}{6}\right)$, queremos encontrar o outro ponto da interseção $C \cap r$, em função do coeficiente angular da reta r, de equação

$$r : y = \frac{kx}{3} + \frac{k}{6} + \frac{1}{6}.$$

Substituindo a equação da reta r na equação da cônica C temos

$$9\Big(\frac{2kx+k+1}{6}\Big)^2 = -11x^2 - 14x - 4$$
$$9\Big(\frac{4k^2x^2+4k^2x+4kx+k^2+2k+1}{36}\Big) = -11x^2 - 14x - 4$$

Simplificando, obtemos uma equação quadrática em x:

$$(11+k^2)x^2+(k^2+k+14)x+\frac{k^2}{4}+\frac{k}{2}+\frac{17}{4}=0.$$

cujo discriminante $\Delta=(k^2+k+14)^2-4(11+k^2)\left(\frac{k^2}{4}+\frac{k}{2}+\frac{17}{4}\right)=(k+3)^2$. *Logo os pontos dessa interseção são*

$$x_1=\frac{-1}{2}, \qquad y_1=\frac{1}{6}$$
$$x_2=-\frac{k^2+2k+17}{22+2k^2}, \qquad y_2=-\frac{k^2+6k-11}{6k^2+66}.$$

A respectiva solução em função de k para (2) é

$$(r,s,t)=\Big(\frac{2k^2+6k+20}{3k^2+33}, \frac{k^2+31}{3k^2+33}, \frac{4(2k^4-3k^3+28k^2-75k+80)}{(3k^2+33)^2}\Big).$$

Mais geralmente, sempre que u satisfaz as hipóteses do Lema 4.2.11, pode-se encontrar uma solução paramétrica da equação $r^4+s^4+t^2=1$, com r,s de grau 2 e t de grau 4 com denominador quadrado.

4.2.1 A superfície $S_1: r^4+s^4+t^4=1$

Buscar soluções racionais para a equação $r^4+s^4+t^4=1$ é equivalente a buscar solução racional de $r^4+s^4+t^2=1$, com a restrição adicional que t é um quadrado. Substituindo t por $\pm t^2$ em (4.8) e (4.9) temos o seguinte sistema

$$\begin{aligned} r=x+y, s=x-y,& \\ (2m^2+n^2)y^2=-(6m^2-8mn+3n^2)x^2-2(2m^2-n^2)x-2mn& \\ \pm(2m^2+n^2)t^2=4(2m^2-n^2)x^2+8mnx+(n^2-2m^2).& \end{aligned} \tag{4.14}$$

Exemplo 4.2.13. *Tomando $(m,n)=(0,1)$, obtemos as cônicas*

$$C_1: y^2=-3x^2+2x,\ C_{\pm 2}: \pm t^2=1-4x^2.$$

O ponto $(0,0)$ claramente pertence a C_1. Considerando a reta l de equação $y=kx$, encontramos o segundo ponto da interseção $C_1\cap l$, cujas coordenadas em função de k são dadas por

$$(x,y)=\Big(\frac{2}{k^2+3}, \frac{2k}{k^2+3}\Big).$$

Substituindo na equação de $C_{\pm 2}$ temos

$$\pm t^2=\frac{k^4+6k^2-7}{(k^2+3)^2}.$$

Pondo $z = (k^2 + 3)t$, temos duas curvas de gênero um de equações $\pm z^2 = k^4 + 6k^2 - 7$, já que o polinômio $g(k, z) = k^4 + 6k^2 - 7 = (k^2 + 7)(k^2 - 1)$ não possui raízes múltiplas. Dessa forma, obtemos duas curvas elípticas, cujas formas de Weierstrass são dadas por

$$\begin{aligned} Y^2 &= X^3 + X^2 + 2 \\ Y^2 &= X^3 + X^2 - 2. \end{aligned} \tag{4.15}$$

obtida através da mudança de variáveis

$$k = 1 - \frac{4}{1 \pm X}, z = \frac{8Y}{(1 \pm X)^2}.$$

Em uma análise inicial, vemos que os pontos $(\pm 1, 0) \in E_1(\mathbb{Q})$ correspondem as soluções triviais

$$\begin{aligned} r = x + y = \frac{2 + 2k}{k^2 + 3} = \frac{X^2 - 1}{X^2 + 3} = 0; \\ s = x - y = \frac{2 - 2k}{k^2 + 3} = \frac{\pm X + 2}{X^2 + 3} = 1; \\ \pm t^2 = \frac{k^4 + 6k^2 - 7}{(k^2 + 3)^2} = -\frac{4(X^3 + X \pm 2)}{(X^2 + 3)^2} = 0; \end{aligned}$$

e $(1, \pm 2) \in E_1(\mathbb{Q})$ corresponde ao ponto $(r, s, t) = (0, 0, 1)$ em S_1. Desejamos encontrar soluções não triviais da equação $r^4 + s^4 + t^4 = 1$, para isto, devemos escolher valores diferentes para m e n em (4.14).

Lema 4.2.14. *A cônica da equação (4.14) tem infinitos pontos racionais (x, t) se os números $R(2m^2 - 2mn + n^2)$, $R(2m^2 + n^2)$ e $R(2m^2 + 2mn + n^2)$ são todos produtos de primos congruentes a 1 módulo 8.*

Demonstração. Analogamente, vamos colocar a equação (4.14) na forma

$$aX^2 + bY^2 + cZ^2 = 0.$$

Seja $X = [4mn + (n^2 - 2m^2)]$. Então $X^2 = (n^2 - 2m^2)[(n^2 - 2m^2) + 8mnx + 4(2m^2 - n^2)x^2] + (16m^4 + 4n^4)x^2$. Substituindo (4.14) na equação acima temos

$$X^2 \pm (2m^2 - n^2)(2m^2 + n^2)t^2 - 4(2m^2 - 2mn + n^2)(2m^2 + 2mn + n^2)x^2 = 0. \tag{4.16}$$

Tomando $\alpha = S((2m^2 - n^2)(2m^2 + n^2)) = S(4m^4 - n^4)$, $\beta = S((2m^2 - 2mn + n^2)(2m^2 + 2mn + n^2) = S(4m^4 + n^4)$, $a = R(4m^4 - n^4)$ e $b = R(4m^4 + n^4)$, a equação (4.16) fica na forma

$$X^2 \pm (a\alpha^2)t^2 - 4(b\beta^2) = 0.$$

Fazendo $Y = \alpha t$ e $Z = \beta x$, colocamos 4.16 na forma

$$X^2 \pm aY^2 - 4bZ^2 = 0. \tag{4.17}$$

Pelo teorema de Legendre, a equação acima terá solução inteira não trivial se e somente se $\pm(4m^4 - n^4)$ é um resíduo quadrático módulo cada fator primo de $R(2m^2 \pm 2mn + n^2)$ e $4m^4 + n^4$ é um resíduo quadrático módulo $R(2m^2 \pm n^2)$. Se $\pm(4m^4 - n^4)$ for um resíduo quadrático módulo $R(2m^2 \pm 2mn + n^2)$ e $4m^4 + n^4$ for um resíduo quadrático módulo $R(2m^2 \pm n^2)$ então a condição acima é sempre satisfeita. Temos que

$$4m^4 - n^4 \equiv (2m^2 - 2mn + n^2)(2m^2 + 2mn + n^2) \equiv 2n^4 mod(4m^4 + n^2);$$
$$n^4 - 4m^4 \equiv -(2m^2 - 2mn + n^2)(2m^2 + 2mn + n^2) \equiv -2n^4 mod(4m^4 + n^2).$$

Logo, devemos ter 2 e -2 resíduos quadráticos módulo cada fator primo p_i na fatoração $R(2m^2 - 2mn + n^2)$. É necessário que m, n também satisfaçam as seguintes condições

$$4m^4 + n^4 \equiv 2n^4 \equiv -(2nm)^2 mod(2m^2 + n^2)$$
$$4m^4 + n^4 \equiv -(2mn)^2 mod(2m^2 + n^2).$$

Então -1 e 2 deverão ser resíduos quadráticos módulo cada fator primo de $R(2m^2 + n^2)$. A última condição $4m^4 + n^4 \equiv (2nm)^2 mod(2m^2 - n^2)$ é sempre satisfeita. Como foi visto no lema 4.2.6, todos esses primos são congruentes a 1 módulo 8.

□

Nosso interesse é encontrar inteiros m, n relativamente primos, com m não negativo e n ímpar, que satisfaçam as condições de ambos os lemas (4.2.11) e (4.2.14), para então obtermos uma solução inteira não trivial para a equação diofantina estudada. Os pares $(m, n) = (0, 1)$, $(4, -7), (8, -5), (12, 5), (20, -1)$ satisfazem as condições dos lemas 4.2.14 e 4.2.11, em particular, m é par: o número $2m^2 + n^2$ é da forma $8w + 1$, para w inteiro arbitrário. Então $m^2 = (4w + k)$, sendo k um número par, pois $1 - n^2 = 2k$ e logo $(1 - n)(1 + n) = 2k$. Como n é ímpar, $1 \pm n$ é par, segue que k e m são números pares. Uma outra observação é que os pontos da forma $(2n, n)$ não satisfazem as hipóteses dos lemas 4.2.11 e 4.2.14, pois tomando $m = 2n$, temos que $2m^2 + 2mn + n^2 = 8n^2 + 4n^2 + n^2 = 13n^2$, logo, $R(13n^2) = 13 \not\equiv 1\ mod(8)$.

Tomando $(m, n) = (8, -5)$ temos $R(2m^2 + n^2) = R(153) = 17$ e $R(2m^2 + 2mn + n^2) = R(73) = 73$, logo as condições dos Lemas 4.2.11 e 4.2.14 são satisfeitas. Para esses valores, as respectivas cônicas são dadas por

$$\begin{aligned} C_f &: 153y^2 = -779x^2 - 206x + 80 \\ C_{\pm g} &: \pm 153t^2 = 412x^2 - 320x - 103. \end{aligned} \tag{4.18}$$

O ponto $\left(\frac{3}{14}, \frac{1}{42}\right)$ pertence à curva C_f. Queremos encontrar o outro ponto na interseção $C_f \cap s$, onde s é a reta de equação $y = \frac{14kx-3k+1}{42}$. Substituindo na equação da cônica C_f, obtemos uma equação quadrática em x:

$$(17k^2 + 779)x^2 - \Big(\frac{51k^2}{7} - \frac{17k}{7} + 206\Big)x + \frac{153k^2}{196} + \frac{51k}{98} - \frac{1566}{196} = 0$$

cuja solução em função do coeficiente k é dada por

$$(x, y) = \Big(\frac{51k^2 - 34k - 5221}{14(17k^2 + 779)}, \frac{17k^2 + 7558k - 779}{42(17k^2 + 779)} \Big).$$

Substituindo o valor da coordenada x na equação de $C_{\pm g}$ temos

$$\pm 21(17k^2 + 779)^2 t^2 = -4(31.790k^4 - 4.267k^3 + 1.963.180k^2 - 974.003k - 63.237.532). \tag{4.19}$$

Em $\mathbb{Z}_3$, o lado direito da equação acima fica na forma

$$\begin{aligned} -4(31790k^4 - 4267k^3 + 1963180k^2 - 974003k - 63237532) &\equiv 4k^4 - 2k^3 + 2k^2 + 2k - 2 \ mod(3). \\ &\equiv k^4 + k^3 - k^2 - k + 1 \ mod(3) \\ &\equiv (k^2 - k - 1)^2 \ mod(3). \end{aligned}$$

Para manter pontos (x, y) em coordenadas racionais, devemos escolher o sinal positivo em (4.19). Vamos colocar (4.19) da forma $Y^2 = ax^4 + bx^3 + cx^2 + dx + e$, para isto, fazemos a seguinte mudança de variáveis:

$$X = \frac{k+2}{7}, \quad Y = \frac{3}{14}(17k^2 + 779)t;$$

$$\begin{aligned} Y^2 &= \frac{9t^2}{196}(17k^2 + 779)^2; \\ 31790k^4 &= 76327790X^4 + 87231760X^3 + 37385040X^2 + 7120960X + 508640 \\ -4267k^3 &= -1463581X^3 + 1254498X^2 - 358428X + 34136; \\ 1.963.180k^2 &= 96195820X^2 - 54969040X + 7852720; \\ -974003k &= \ 1948006 - 6818021X. \end{aligned}$$

Assim,

$$\frac{4.7^3}{3}Y^2 = 21t^2(17k^2 + 779) \text{ e } -4(31790k^4 - 4267k^3 + 1963180k^2 - 974003k - 63237532) =$$

$$-305311160X^4-348927040X^3-149540160X^2-28483840X-2034560+5854324X^3-5017992X^2$$

$$+1433712X-136544-384783280X^2+219876160X-31410880+27272084X-7792024+252950128$$

$$= -305311160X^4 - 343072716X^3 - 539341432X^2 + 220098116X + 211576120$$

A equação (4.19) fica na forma

$$Y^2 = -31790X^4 + 36941X^3 - 56158X^2 + 28849X + 22030 \tag{4.20}$$

Os pontos

$$P_{\pm} = \Big(-\frac{31}{467}\ ,\ \pm\frac{30731278}{467^2}\Big)$$

satisfazem a equação acima. Assim, a equação (4.20) define uma curva E de gênero 1 que possui pontos racionais, logo é uma curva elíptica. Temos que

$$X = \frac{k+2}{7} \ \Rightarrow k = -\frac{1151}{467}.$$

Substituindo nas cônicas de equação (4.18), temos

$$(x, y) = \Big(\frac{37600080}{6871891}\ ,\ -\frac{10739600}{20615673}\Big).$$

A solução racional para a equação que define a superfície S_1 é dada por

$$(r, s, t) = \Big(-\frac{18796760}{20615673}\ ,\ \frac{2682440}{20615673}\ ,\ \frac{15365639}{20615673}\Big).$$

Por meio dessa construção, obtemos o primeiro contraexemplo para o caso $n = 4$ da Conjectura de Euler:

$$2682440^4 + 15365639^4 + 18796760^4 = 20615673^4.$$

4.2.2 Considerações Finais

Posteriormente, Roger Frye encontrou os menores números inteiros positivos satisfazendo a equação

$a^4 + b^4 + c^4 = e^4$, a saber

$$95800^4 + 217519^4 + 414560^4 = 422481^4.$$

Tal solução foi obtida por meio de um programa computacional, sendo executado em várias máquinas conectadas por cerca de 100 horas, após uma série de procedimentos aritméticos e algébricos, como por exemplo, eliminar fatores comuns de a, b e c e tomando e como sendo

um número ímpar não divisível por 5. Além disso, ele preferiu estudar outra representação da equação acima, $a^4 + b^4 = e^4 - c^4$, com a, b números inteiros divisíveis por 5. Tal solução pode ser obtida no método apresentado na seção anterior, se considerarmos $(m, n) = (20, -9)$ na parametrização (4.14). Ele continuou sua pesquisa e descobriu que esta solução é a única satisfazendo $e < 10^6$.

A partir dos pontos $P_\pm$ na curva elíptica E, podemos usar a lei de grupo dessa curva para encontrar novos pontos. Contudo, definimos a lei de grupo de uma curva elíptica na forma de Weierstrass, no nosso caso, a curva elíptica E não está definida nesse formato. Poderíamos fazer uma mudança de variáveis e colocar a equação de E na forma de Weierstrass, o que será um trabalho árduo, devido aos coeficientes grandes dessa equação. É possível computar a lei de grupo diretamente em termos das coordenadas x e y, tomando em vez de retas, parábolas

$y = ax^2 + bx + c$, tangentes à curva E. Essa construção pode ser encontrada em [2]. Se um ponto Q é obtido a partir dos pontos $P_\pm$ nessa lei de adição, então a próxima questão natural é determinar a ordem do ponto Q. O teorema de Masur afirma que se $[n]\mathbb{Q} \neq \mathcal{O}$ para $n = 2, 3, ..., 12$, então esse ponto tem ordem infinita. Nesse caso, obtemos uma sequência infinita $Q, 2Q, 3Q, ...$ de pontos em E, consequentemente, pelo método apresentado na seção anterior, obtemos uma infinidade de soluções inteiras positivas para a equação $a^4 + b^4 + c^4 = e^4$.

Para alcançar nosso objetivo específico, nos preocupamos apenas em buscar pontos racionais situados na superfície S_1. Com um pouco mais de trabalho demonstra-se, que os pontos racionais na superfície S_1 formam um conjunto denso no conjunto dos pontos reais de S_1 (Ver [4], pág. 833).

Capítulo 5

Soluções para a equação diofantina $a^4 + b^4 + c^4 + d^4 = e^4$

5.1 Considerações Iniciais

Equações diofantinas da forma

$$\sum_{i=1}^{m} a_i^k = \sum_{j=1}^{n} b_j^k, \tag{5.1}$$

vem sendo estudadas há anos por muitos matemáticos [3], sendo classificadas de acordo com as seguintes abordagens:

- $k > m + n$;
- $k = m + n$;
- $k < m + n$;

A chamada Conjectura Estendida de Euler, afirma que não existem soluções (k, n, m) para tal equação quando $k > m + n$. Até o momento, não são conhecidos resultados numéricos para essa abordagem. Em relação a segunda abordagem, segue alguns dos resultados numéricos conhecidos:

- $(4, 1, 3) : 2.682.440^4 + 15.365.639^4 + 18.796.760^4 = 20.615.673^4$ (Elkies, 1988).
- $(4, 2, 2) : 59^4 + 158^4 = 133^4 + 134^4$ (Euler, 1750).

[3] Ver [12] para conhecer alguns dos principais resultados publicados.

- $(5, 1, 4) : 27^5 + 84^5 + 110^5 + 133^5 = 144^5$ (Lander, Parkin, 1967).

- $(8, 3, 5) : 81^8 + 539^8 + 966^8 = 158^8 + 310^8 + 481^8 + 725^8 + 954^8$ (Chase, 2000).

Para a terceira abordagem, segue alguns dos principais resultados publicados:

- $(4, 1, 4) : 30^4 + 120^4 + 272^4 + 315^4 = 353^4$ (Norrie, 1911).

- $(5, 1, 5) : 19^5 + 43^5 + 46^5 + 47^5 + 67^5 = 72^5$ (Lander, Parkin, 1967).

- $(7, 1, 7) : 127^7 + 258^7 + 266^7 + 413^7 + 430^7 + 439^7 + 525^7 = 568^7$(Dodrill, 1999).

No presente capítulo, trataremos da segunda abordagem: Vamos buscar novas soluções para a equação $a^4 + b^4 + c^4 + d^4 = e^4$, mais especificamente, exibiremos o método desenvolvido por Lee W. Jacobi e Daniel Madden para gerar uma sequência infinita de números inteiros positivos satisfazendo tal equação, considerando o caso particular em que $e = (a + b + c + d)$. Isto foi possível devido a solução particular encontrada por Simcha Brudno em 1964,

$$5400^4 + 1770^4 + 2634^4 + 955^4 = 5491^4,$$

que também satisfaz

$$5400 + 1770 + 955 = 2634 + 5491.$$

Isto significa que $(5400, 1770, -2634, 955)$ é solução da equação diofantina

$$a^4 + b^4 + c^4 + d^4 = (a + b + c + d)^4. \tag{5.2}$$

Vale ressaltar que até antes da publicação de Jacobi e Madden em 2008, não era conhecido um método que gerasse uma família de soluções inteiras positivas para tal equação, considerando todas as variáveis diferentes de zero. Faremos isso da seguinte forma: vamos mostrar que os números inteiros que satisfazem a equação (5.2) estão associados com os pontos racionais em uma família de curvas em $\mathbb{P}^2$. Sob certas condições, vamos reconhecer cada curva nessa família como uma curva elíptica e então usaremos o teorema de Mazur para mostrar que se um ponto nessa curva não é de torção, ele pode ser usado para gerar uma sequência infinita de outros pontos racionais na curva, como consequência, obtemos uma infinidade de soluções inteiras positivas para a equação (5.2).

Uma família de soluções para a equação

$a^4 + b^4 + c^4 + d^4 = (a + b + c + d)^4$

Seja $(5400 : 1770 : -2634 : 955)$ uma solução particular de (5.2). Vamos iniciar reescrevendo a hipersuperfície definida pela equação (5.2) como sendo a interseção de duas superfícies quadráticas. Faremos isso a partir da identidade

$$\alpha^4 + \beta^4 + (\alpha + \beta)^4 = 2(\alpha^2 + \alpha\beta + \beta^2)^2. \tag{5.3}$$

Reescrevendo (5.2) na forma

$$\begin{aligned} a^4+b^4+(a+b)^4+c^4+d^4+(c+d)^4 &= 2a^4+4a^3b+6a^2b^2+4ab^3+2b^4+2c^4+4c^3d+6c^2d^2+4cd^3+2d^4 \\ &= (a+b)^4 + (c+d)^4 + (a+b+c+d)^4, \end{aligned}$$

e aplicando a identidade (5.3), a equação (5.2) fica na forma

$$\begin{aligned} &(a^2 + ab + b)^2 + (c^2 + cd + d)^2 = \\ &a^4 + 2a^3b + a^2b^2 + 2a^2b + 2ab^2 + b^2 + c^4 + 2c^3d + c^2d^2 + 2c^2d + 2cd^2 + d^2 \\ &= ((a + b)^2 + (a + b)(c + d) + (c + d)^2)^2. \end{aligned}$$

Segue que

$$\begin{aligned} &(c^2 + cd + d)^2 = ((a + b)^2 + (a + b)(c + d) + (c + d)^2)^2 - (a^2 + ab + b)^2 = \\ &((a + b)^2 + (a + b)(c + d) + (c + d)^2 + (a^2 + ab + b))((a + b)^2 + (a + b)(c + d) + (c + d)^2 \\ &- (a^2 + ab + b)) \end{aligned} \tag{5.4}$$

Introduzindo um novo parâmetro μ, dividimos a equação (5.4) em duas :

$$\begin{aligned} c^2 + cd + d^2 &= \mu((a + b)^2 + (a + b)(c + d) + (c + d)^2 - a^2 - ab - b^2) \\ c^2 + cd + d^2 &= \frac{1}{\mu}((a + b)^2 + (a + b)(c + d) + (c + d)^2 + a^2 + ab + b^2). \end{aligned} \tag{5.5}$$

A equação (5.5) representa uma família de superfícies quadráticas, assim, a interseção dessas duas superfícies dadas por um mesmo valor do parâmetro μ é uma curva projetiva. Dessa maneira, temos uma família de curvas parametrizadas por um único parâmetro μ e uma solução simultânea para ambas equações em (5.5), dada por

$$a_0 = 5400; \quad b_0 = 1770; \quad c_0 = -2634; \quad d_0 = 955.$$

Para esse ponto particular, o valor de μ acima é

$$\mu_0 = \frac{961}{61}.$$

Assim, temos um ponto racional na interseção dessas superfícies quadráticas:

$$c^2+2cd+d^2=\mu_0(ab+ac+bc+ad+bd+c^2+2cd+d^2)$$
$$\mu_0(c^2+2cd+d^2)=2a^2+3ab+2b^2+ac+bc+ad+bd+c^2+2cd+d^2,$$

e logo, suspeitamos que essa interseção seja uma curva elíptica. Para encontrar a equação dessa curva explicitamente, vamos fazer a seguinte mudança de variáveis

$$a=2z+2w;\quad b=2z-2w;\quad c=-x-y-z;\quad d=x-y-z.$$

As equações das duas superfícies quadráticas dadas por (5.5) ficam respectivamente

$$\begin{aligned}61(x^2+3y^2+6yz+3z^2)&=961(4y^2-4w^2)\\ 961(x^2+3y^2+6yz+3z^2)&=61(4w^2+4y^2+24z^2).\end{aligned}\tag{5.6}$$

Multiplicando a primeira equação pelo valor obtido para μ_0 e subtraindo a segunda, temos o seguinte sistema:

$$61x^2-3661y^2+366yz+183z^2+3844w^2=0 \tag{5.7}$$

$$459900y^2-11163z^2-463621w^2=0. \tag{5.8}$$

A correspondente solução para esse novo sistema de equações é o ponto

$$(x_0:y_0:z_0:w_0)=\Big(\frac{3589}{2},-953,\frac{3585}{2},\frac{1815}{2}\Big).$$

Como a segunda equação envolve apenas três das variáveis, ela representa uma cônica em $\mathbb{P}^2$. Queremos encontrar o conjunto das soluções paramétricas racionais para (5.8), a partir do ponto conhecido $(y_0:z_0:w_0)$ e do coeficiente angular de uma reta passando por esse ponto. No plano afim $w=1$, a solução da equação (5.8) é o ponto

$$(y_0',\ z_0')=\Big(-\frac{1906}{1815},\ \frac{3585}{1815}\Big).$$

Intersectando a curva afim $C\colon 459900y^2-11163z^2-463621=0$ com a reta $z=m(y-y_0')+z_0'$, obtemos uma equação quadrática em y:

$$(459900-11163m^2)y^2-\Big(40019355m+\frac{42553356}{1815}m^2\Big)y-11163\delta-\tau$$

onde

$$\delta=\Big(\frac{3632836}{3294225}m^2+\frac{13666020}{3294225}m\Big);\ \tau=\frac{1567825236993}{3294225}.$$

Tomando $m = \frac{s}{t}$, $t \neq 0$, as equações paramétricas da curva projetiva de equação (5.8) são:

$$\begin{aligned} y_1 &= -6(146094900t^2 + 13339785st + 3546113s^2) \\ z_1 &= 45(36638700t^2 + 38958640st + 889319s^2) \\ w_1 &= 5445(153300t^2 - 3721s^2). \end{aligned} \tag{5.9}$$

Substituindo os valores de y_1, z_1, w_1 obtidos acima em (5.8), obtemos a equação

$$\begin{aligned} &f(s,t) = x^2t^2, \text{ onde} \\ &f(s,t) = 40064007^2s^4 + 26478277616573460s^3t - 3598879905807952500s^2t^2 \\ &+10908680351036580000st^3 + 1650581100^2t^4. \end{aligned} \tag{5.10}$$

A equação (5.10) define uma curva elíptica em $\mathbb{P}^2$ se e somente se, o polinômio $f(s,1)$ não possui raízes múltiplas. Como os coeficientes são grandes, usamos o software Wolfram para verificar que $f(s,1)$ não possui raízes múltiplas.

Dessa forma a equação (5.10) define uma curva elíptica E e todo ponto racional em E fornece uma solução inteira para a equação $a^4 + b^4 + c^4 + d^4 = (a+b+c+d)^4$, pois

$$\begin{aligned} a &= 2z_1 + 2w_1 = 39517020s^2 + 3506277600st + 4966920000t^2 \\ b &= 2z_1 - 2w_1 = 120560400s^2 + 3506277600st + 1628046000t^2 \\ c &= -x - y_1 - z_1 = -18742677s^2 - 1673100090st - 772172100t^2 - tx \\ d &= x - y_1 - z_1 = -18742677s^2 - 1673100090st - 772172100t^2 + tx. \end{aligned}$$

Em particular, os pontos $P_\pm = (s_0 : x_0 : t_0) = (0 : \pm 1650581100 : 1)$ satisfazem (5.10). Assim, temos uma curva elíptica com dois pontos racionais conhecidos. Nosso próximo passo é usar a lei de grupo para encontrar novos pontos em E.

Lema 5.1.1. *Se $(x_1 : y_1 : z_1)$ é uma solução da equação $z^2y^2 = F(x,z) = \alpha_4x^4 + \alpha_3x^3z + \alpha_2x^2z^2 + \alpha_1xz^3 + \alpha_0z^4$, então também é solução*

$$\begin{aligned} x_2 &= (64x_1y_1^6z_1^6\gamma^4 - q_0^2x_1 - 64y_1^6z_1^6\gamma^3 + 8q_0y_1^2z_1^2\gamma_1)(64y_1^6z_1^6\gamma^4 - q_0^2) \\ y_2 &= 9q_0y_1(q_0\gamma_1 - 8y_1^4z_1^4\gamma^3)^2 + 4y_1\gamma_1(q_0\gamma_1 - 8y_1^4z_1^4\gamma^3)(64y_1^6z_1^6\gamma^4 - q_0^2) + y_1(64y_1^6z_1^6\gamma^4 - q_0^2)^2 \\ z_2 &= z_1(64y_1^6z_1^6\gamma^4 - q_0^2)^2, \end{aligned}$$

onde

$$\begin{aligned}
\gamma_1 &= F'(x_1,z_1) = 4\alpha_4 x_1^3 + 3\alpha_3 x_1^2 z_1 + 2\alpha_2 x_1 z_1^2 + \alpha_1 z_1^3 \\
\gamma_2 &= \frac{F''(x_1,z_1)}{2} = 6\alpha_4 x_1^2 + 3\alpha_3 x_1 z_1 + \alpha_2 z_1^2 \\
\gamma_3 &= \frac{F'''(x_1,z_1)}{3!} = 4\alpha_4 x_1 + \alpha_3 z_1 \\
\gamma_4 &= \frac{F''''(x_1,z_1)}{4!} = \alpha_4 \\
q_0 &= 4y_1^2 z_1^2 \gamma_2 - \gamma_1^2.
\end{aligned} \tag{5.11}$$

Demonstração. Sejam $g(x) = \alpha_4 x^4 + \alpha_3 x^3 + \alpha_2 x^2 + \alpha_1 x + \alpha_0$, $f(x,y) = y^2 - g(x)$, E a curva elíptica definida pelo polinômio f e $P = (x_0, y_0)$ um ponto em E. Consideremos o polinômio de Taylor de $g(x)$ em torno de x_0

$$y^2 = \beta_4(x-x_0)^4 + \beta_3(x-x_0)^3 + \beta_2(x-x_0)^2 + \beta_1(x-x_0) + \beta_0,$$

onde

$$\begin{aligned}
\beta_0 &= g(x_0) = y_0^2 \\
\beta_1 &= g'(x_0) = 4\alpha_4 x_0^3 + 3\alpha_3 x_0^2 + 2\alpha_2 x_0 + \alpha_1 \\
\beta_2 &= \frac{g''(x_0)}{2} = 6\alpha_4 x_0^2 + 3\alpha_3 x_0 + \alpha_2 \\
\beta_3 &= \frac{g'''(x_0)}{3!} = 4\alpha_4 x_0 + \alpha_3 \\
\beta_4 &= \frac{g''''(x_0)}{4!} = \alpha_4 \\
\frac{dy}{dx} &= \frac{g'(x)}{2y} \\
\frac{d^2y}{dx^2} &= \frac{2y^2 g''(x) - (g'(x))^2}{4y^3} \\
m_0 &= \frac{dy}{dx}(x_0,y_0) = \frac{\beta_1}{2y_0} \\
p_0 &= \frac{d^2y}{dx^2}(x_0,y_0) = \frac{4y_0^2\beta_2 - \beta_1^2}{4y_0^3}\ .
\end{aligned}$$

O polinômio obtido pela interseção da parábola

$$C\colon\ y = \frac{p_0}{2}(x-x_0)^2 + m_0(x-x_0) + y_0$$

com a curva E é dado por

$$\Big(\beta_4 - \frac{p_0^2}{4}\Big)(x-x_0)^4 + (\beta_3 - p_0 m_0)(x-x_0)^3.$$

Concluímos que $(E,C)_P = 3$ e a multiplicidade de interseção do ponto P' de coordenadas

$$\Big(-\frac{4\beta_3 - 4p_0m_0}{4\beta_4 - p_0^2} + x_0, \quad \frac{p_0}{2}\Big(\frac{4\beta_3 - 4p_0m_0}{4\beta_4 - p_0^2} \Big)^2 - m_0\Big(\frac{4\beta_3 - 4p_0m_0}{4\beta_4 - p_0^2} \Big) + y_0\Big)$$

é $(E, C)_{P'} = 1$. Um ponto $(x_1 : y_1 : z_1)$ em $\mathbb{P}^2$ é identificado com o ponto $P = (x_0, y_0)$ no plano afim por

$$(x_0, y_0) = \Big(\frac{x_1}{z_1}, \frac{y_1}{z_1}\Big).$$

Fazendo essa mudança de coordenadas, temos

$$\begin{aligned}
\beta_0 &= \Big(\frac{y_1}{z_1}\Big)^2 \\
\beta_1 &= 4\alpha_4\Big(\frac{x_1}{z_1}\Big)^3 + 3\alpha_3\Big(\frac{x_1}{z_1}\Big)^2 + 2\alpha_2\Big(\frac{x_1}{z_1}\Big) + \alpha_1 \\
\beta_2 &= 6\alpha_4\Big(\frac{x_1}{z_1}\Big)^2 + 3\alpha_3\Big(\frac{x_1}{z_1}\Big) + \alpha_2 \\
\beta_3 &= 4\alpha_4\Big(\frac{x_1}{z_1}\Big) + \alpha_3 \\
\beta_4 &= \alpha_4
\end{aligned} \tag{5.12}$$

$$\begin{aligned}
\gamma_1 &= z_1^3\beta_1 \\
\gamma_2 &= z_1^2\beta_2 \\
\gamma_3 &= z_1\beta_3 \\
\gamma_4 &= \beta_4 \\
q_0 &= 4y_1^3z_1^3p_0.
\end{aligned} \tag{5.13}$$

Vamos considerar a curva E em $\mathbb{P}^2$ obtida pelo polinômio $F = f^*$. Para obtermos um ponto $P_2 = (x_2 : y_2 : z_2)$ em E, inicialmente encontramos o correspondente ponto de coordenadas afins $P_2' = \Big(\frac{x_2}{z_2}, \frac{y_2}{z_2}\Big)$ na parte afim de E. Substituindo os valores obtidos em (5.12) e (5.13) e tomando $z_2 = 4\beta_4 - p_0^2$ nas coordenadas do ponto P'

$$\Big(-\frac{4\beta_3 - 4p_0m_0}{4\beta_4 - p_0^2} + x_0, \quad \frac{p_0}{2}\Big(\frac{4\beta_3 - 4p_0m_0}{4\beta_4 - p_0^2} \Big)^2 - m_0\Big(\frac{4\beta_3 - 4p_0m_0}{4\beta_4 - p_0^2} \Big) + y_0\Big)$$

na interseção $C \cap E$, segue que

$$\begin{aligned}
z_2 &= z_1(64y_1^6z_1^6\gamma_4 - q_0^2); \\
\frac{x_2}{z_2} &= \frac{x_1}{z_1} + \frac{(8q_0y_1^2z_1^2\gamma_1 - 64y_1^6z_1^6\gamma_3)(64y_1^6z_1^6\gamma_4 - q_0^2)}{z_2}\,; \\
\frac{y_2}{z_2} &= \frac{y_1}{z_1} + \frac{8q_0y_1(q_0y_1 - 8y_1^4z_1^4\gamma_3)^2 + 4y_1\gamma_1(q_0\gamma_1 - 8y_1^4z_1^4\gamma_3)(64z_1^6y_1^6\gamma_4 - q_0^2)}{z_2}\,;
\end{aligned}$$

e logo,

$$x_2 = (64x_1y_1^6z_1^6\gamma^4 - q_0^2x_1 - 64y_1^6z_1^6\gamma^3 + 8q_0y_1^2z_1^2\gamma_1)(64y_1^6z_1^6\gamma^4 - q_0^2)$$
$$y_2 = 9q_0y_1(q_0\gamma_1 - 8y_1^4z_1^4\gamma^3)^2 + 4y_1\gamma_1(q_0\gamma_1 - 8y_1^4z_1^4\gamma^3)(64y_1^6z_1^6\gamma^4 - q_0^2) + y_1(64y_1^6z_1^6\gamma^4 - q_0^2)^2$$
$$z_2 = z_1(64y_1^6z_1^6\gamma^4 - q_0^2)^2.$$

□

Utilizaremos o lema acima para gerar uma sequência de novos pontos racionais na curva elíptica E de equação (5.10), a partir dos pontos conhecidos

$$P_\pm = (s_0 : x_0 : t_0) = (0 : \pm 1650581100 : 1).$$

A fim de facilitar os cálculos, devido aos coeficientes grandes na equação (5.10), vamos considerar E definida sobre um corpo $\mathbb{F}_p$, onde p é um número primo escolhido de maneira conveniente. Isto permite definir um grupo finito $E(\mathbb{F}_p)$ cuja estrutura é mais simples de analisar do que a estrutura do grupo $E(\mathbb{Q})$. Escolhendo $p = 71$, é possível identificar 18 pontos racionais distintos em $E(\mathbb{F}_{71})$.

As coordenadas de P_+ em $\mathbb{F}_{71}$ são dadas por

$$(0 : 1650581100 : 1) \equiv (0 : 9 : 1)\ mod\ (71)$$

Aplicando o lema 5.2.1 temos

$$\begin{aligned}
&\gamma_1 = \alpha_1 = 1090868035103658000 \equiv 28\ mod(71)\\
&\gamma_2 = \alpha_2 = -3598879905807952500 \equiv -55\ \equiv 16\ mod(71)\\
&\gamma_3 = \alpha_3 = 26478277616573460 \equiv 48 \equiv -23\ mod(71)\\
&\gamma_4 = \alpha_4 = 1605124656896049 \equiv 12\ mod(71)\\
&q_0 = 4400 \equiv 69 \equiv -2\ mod(71)
\end{aligned} \tag{5.14}$$

As coordenadas do novo ponto obtido no lema a partir de ponto $(0 : 9 : 1)$ são dadas por

$$s = (64.9^6.23 - 16.9^2.28)(64.9^6.12 - 4) = 319270647317630976 \equiv 53\ mod(71)$$

$$\begin{aligned}
x &= -16.9(-56 + 8.9^4.23)^2 + 36.28(-56 + 8.9^4.23)(64.9^6.12 - 4) + 9(64.9^6.12 - 4)^2\\
&= 1995686825442969744 \equiv 64\ mod(71).
\end{aligned}$$

$$t = (64.9^4.12 - 4)^2 = 166583715660195856 \equiv 50\ mod(71)$$

Assim, como temos uma simetria nessa curva, o ponto $(53 : -64 : 50) \in E(\mathbb{F}_{71})$. Prosseguindo dessa forma, obtemos os seguintes pontos:

Tabela 5.1:

s	44	41	47	60	15	39	2
x	± 31	± 1	± 8	± 48	± 41	± 56	± 10
t	24	1	54	8	10	6	15

Como os valores da coordenada t obtidos acima, são todos números diferentes de zero em $\mathbb{F}_{71}$, podemos dividir cada coordenada por t. As respectivas coordenadas racionais são

Tabela 5.2:

s	0	$\frac{53}{50}$	$\frac{11}{6}$	41	$\frac{47}{54}$	$\frac{15}{2}$	$\frac{3}{2}$	$\frac{13}{2}$	$\frac{2}{15}$
x	± 9	$\pm\frac{32}{25}$	$\pm\frac{31}{24}$	± 1	$\pm\frac{2}{27}$	± 6	$\pm\frac{41}{10}$	$\pm\frac{28}{3}$	$\pm\frac{2}{3}$
t	1	1	1	1	1	1	1	1	1

A partir dessa construção obtemos 16 pontos racionais distintos $(s/t : x/t : 1)$ módulo 71, e juntamente com os pontos $(0 : \pm 9 : 1)$, temos 18 pontos distintos em $E(\mathbb{F}_{71})$. Esses pontos (antes da redução módulo 71) são todos distintos e racionais em $E(\mathbb{Q})$. Pelo teorema de Mazur podemos concluir que pelo menos dois desses pontos possui ordem infinita, e logo, a curva elíptica E possui uma infinidade de pontos racionais. Isto significa que o conjunto dos números inteiros positivos satisfazendo $a^4 + b^4 + c^4 + d^4 = (a + b + c + d)^4$ é infinito.

Referências Bibliográficas

[1] S. Brudno. Some new results on equal sums of like powers. *Mathematics of Computation*, 23 (108): 877–880, 1969.

[2] C. Costello and K. Lauter. Group law computations on jacobians of hyperelliptic curves. In *International Workshop on Selected Areas in Cryptography*, 92–117. Springer, 2011.

[3] V. Demjanenko. L. euler's conjecture. *Acta Arith*, 25: 127–135, 1973.

[4] N. D. Elkies. On $a^4 + b^4 + c^4 = d^4$. *Mathematics of Computation*, 825–835, 1988.

[5] K. Ireland and M. Rosen. *A classical introduction to modern number theory*, volume 84. Springer Science & Business Media, 2013.

[6] L. W. Jacobi and D. J. Madden. On $a^4 + b^4 + c^4 + d^4 = (a + b + c + d)^4$. *American Mathematical Monthly*, 115: 220–236, 2008.

[7] J. S. Milne. *Elliptic curves*. BookSurge, 2006.

[8] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106. Springer Science & Business Media, 2009.

[9] H. Stichtenoth. *Algebraic function fields and codes*, volume 254. Springer Science & Business Media, 2009.

[10] I. Vainsencher. *Introdução às curvas algébricas planas*. Impa, 1979.

[11] R. J. Walker. *Algebraic curves*, volume 642. 1950.

[12] E. W. Weisstein. Diophantine Equation - 4th Powers. *Wolfram MathWorld*, 2003.